BYU LAW

Lawyers' Abuse of Technology

Cheryl B. Preston
J. Reuben Clark Law School

103 Cornell Law Review (forthcoming 2018)

J. Reuben Clark Law School, Brigham Young University
Research Paper No. 17-25

Lawyers' Abuse of Technology

Cheryl B. Preston

Contents

INTRODUCTION

Lawyers are highly educated and, allegedly, of higher than average intelligence, but sometimes individual lawyers demonstrate colossal errors in judgment, especially when insufficiently trained in the new and emerging risks involved with the technological age. For

instance, although the internet is a necessary tool for attorneys[1] and is now a prominent feature in the everyday lives of all actors in the legal system, clients, lawyers, and jurors, [2] this technology poses particularized and often unanticipated risks of professional and ethical abuse; risks that are extraordinary both in quantity and intensity.[3] As Harvard's Director of the Center for the Legal Profession warned: We are "only at the forefront of seeing the kind of changes that technology is likely to bring to legal practice," and these changes will "have a profound effect on how we think about regulating lawyers." [4] Unfortunately, the American Bar Association (ABA) missed an opportunity it had with the 20/20 Commission[5] to address meaningful changes in the practice of law wrought by technology.[6] However, the opportunities for unethical and unprofessional behavior in the use of electronic communications and storage cannot be ignored. This Article assesses the risks of technology abuse and proposes a scheme for addressing the professional and ethical problems that have and will continue to accompany the shift to digital lawyering.

---

[1]Sofia Lingos, *Solo and Small Firm*, ABA TECHREPORT 2016, https://www.americanbar.org/groups/law_practice/publications/techreport/2016/solo_small_firm.html ("It is undeniable that technology plays an ever increasing role in our profession and that gaining and maintaining an aptitude early on is necessary."); *see also* Robert Ambrogi, *This Week in Legal Tech: Ethics and Technology Competence*, ABOVE THE L. (July 11, 2016, 3:02 PM), http://abovethelaw.com/2016/07/this-week-in-legal-tech-ethics-and-technology-competence/ (discussing how a firm that is not up-to-date with advances in technology not only faces a competitive disadvantage, but also risks ethical rebuke).

[2] *See* Aaron Street, *Mobile Technology*, ABA TECHREPORT 2016, https://www.americanbar.org/groups/law_practice/publications/techreport/2016/mobile.html (last visited Aug. 10, 2017) (reporting that, "In total, 77% [of survey respondants] say they use the internet for working away from the office. Presumably, these *2016 Survey* respondents assumed 'use the internet' was somehow different than accessing email, because 99% check email while out of the office (89% regularly do)."); RICHARD SUSSKIND, THE END OF LAWYERS? RETHINKING THE NATURE OF LEGAL SERVICES 107 (rev. ed. 2010) ("[I]f you are not [connected to the network and accessible to your client], there is every chance . . . that your competitors will be. The astute lawyer of tomorrow, even if grudgingly, will want to have more or less full-time presence, day and night, on the network, to ensure that any queries from clients will be addressed by their firm rather . . . than another.").

[3] Drew T. Simshaw, *Ethical Implications of Electronic Communication and Storage of Client Information*, RES GESTAE, Dec. 2015, at 9. *See also* Lingos, *supra* note 1 (concluding, "Technological incompetence is not merely a disadvantage, it may be an actual ethical violation.").

[4] DAVID B. WILKINS, *Some Realism About Legal Realism for Lawyers: Assessing the Role of Context in Legal Ethics*, *in* LAWYERS IN PRACTICE: ETHICAL DECISION MAKING IN CONTEXT 25, 34-35 (Lynn Mather & Leslie C. Levin eds., 2012).

[5] *ABA President Carolyn B. Lamm Creates Ethics Commission to Address Technology and Global Practice Challenges Facing U.S. Lawyers*, ABA (Aug. 4, 2009), http:// www.apps.americanbar.org/abanet/media/release/news_release.cfm?releaseid=730 (announcing the creation of the Ethics 20/20 Commission).

[6] *See infra* notes 9-10.

Part I of this Article sets the stage for how to effect change within the existing regulatory scheme to address technoblunders in the legal field. It differentiates various modes of managing and punishing lawyers and briefly explains the role of the First Amendment in regulation of the bar. Part II demonstrates why technologies pose inherent, increased, and intensified risks for incivility, unprofessionalism, and unethical behavior. While the core principles of honesty, respect of others, and confidentiality that are the basis of the Model Rules of Professional Conduct[7] (Model Rules or Rule) and civility standards adopted by individual state, local, and court bar associations do not change with the use of technology, the gaps and ambiguities in the Model Rules make them ineffectual in addressing technology. Lawyers need to be warned, trained, and informed of specific risks to avoid in an area where the risks are new and the any error in judgment can be unusually extensive and severe. In addition, the newness of the technology and the widespread use of email, Facebook, LinkedIn, Twitter, Yelp, Angie's List, AVVO, Lawyers.com, various platforms for bogs and chatrooms, and more warrants efforts to provide more advance guidance alerting of risks and defining safe practices than is necessary with long recognized practice hazards that law students were taught to avoid. Public realization that lawyers are incompetent to use technology, are spying or otherwise deceiving others to get electronic information, or cannot be trusted to confidential information and defense strategy private undermines the entire profession.

Part III provides specific ways that attorneys can and do use technology in ways that are unprofessional and unethical and suggests specific changes to address these issues. Part III is organized in the numerical order of the provision of the Model Rules most relevant to particular harms. The recommendations, however, are not exclusively targeted to changes in the Model Rules. Recognizing the institutional and political difficulty of effecting any changes in the Model

[7] MODEL RULES OF PROF'L CONDUCT (AM. BAR ASS'N 2013).

Rules and the urgency of addressing technology risks, I recommend that changes be made, first, in the various bar associations' professionalism standards and then eventually in the Model Rules. Because drafting consistent and clear professionalism standards can be daunting, I suggest specific language for each of the concerns. The related twin problems of educating lawyers and making certain that regulations are enforced are beyond the scope of this paper.[8]

I. MECHANISMS FOR ADDRESSING TECHNOLOGY ABUSES

Attorney conduct is subject to regulation as a condition to licensure, membership in bar associations, and admittance to practice before particular courts. Like participants in other endeavors, such as the trade in securities and participation in sports competitions, lawyers are subject to rules. The directives and guidelines for conduct in the profession come in various forms.

The profession has made almost no effort to explicate for future guidance how technology may pose particular risks to civility, professionalism, and ethics and how the risks should be addressed. One lawyer stated it this way: "All the rules that the legal profession relies on to instruct lawyer behavior were forged before the emergence of twenty-first century technology. The rule book for this young century has not been written yet . . . ."[9]

One major issue in regulating lawyers is the need to control their willful and intentional violations of ethical and professional standards. Many willful vioations are covered in the Model Rules. But that level of regulation is insufficient. As the technoblunders explicated in this Article demonstrate, at least some attorneys are just negligent in their use of technology and others do not seem to consciously register the misrepresentations inherent in their use of new discovery searches and other methods. In many cases the lawyer should have realized that such conduct

[8] For a discussion of these issues, see Cheryl B. Preston, Professionalism in the Trump Era (forthcoming).
[9] Ken Strutin, *Social Media and the Vanishing Points of Ethical and Constitutional Boundaries*, 31 PACE L. REV. 228, 264 (2011) (citations omitted).

was inappropriate and foreseen the harmful consequences. Other technoblunders are a result of insufficient recognition of new risks.

A. Model Rules of Professional Conduct

The primary mechanism for lawyer regulation is the Rules of Professional Conduct promulgated in model form by the ABA and adopted, typically with few variations, by the various state bar associations.[10] I refer generally to all state versions as Model Rules, unless a variation in a particular state context is noted. The Rules define with some precision the point at which disciplinary action will be taken.[11] But the level of conduct in the Model Rules is set to a low goal – minimal ethics. Even then, continuing and even escalating misbehavior demonstrates that the Model Rules are insufficient to regulate attorney conduct.[12]

The ABA has mechanisms to evaluate where the Model Rules need changes and to propose draft language.[13] Unfortunately, the ABA 20/20 Commission, specifically tasked to address advances in technology, made its only contribution submerged into the comment for

[10] All states have based their ethics rules on the Model Rules, except California, where the Model Rules "may be considered as a collateral source." Diane Karpman, *ABA Model Rules Reflect Technology, Globalization*, CAL. ST. B.J. (Sept. 2012), http://www.calbarjournal.com/September2012/EthicsByte.aspx. In other states, the Model Rules are "considered highly influential guidance when states update their own idiosyncratic Rules of Professional Conduct." *Id.*

[11] Cheryl B. Preston & Hilary Lawrence, *Incentivizing Lawyers to Play Nice: A National Survey of Civility Standards and Options for Enforcement*, 48 U. MICH. J.L. REFORM 701, 710-11 (2015).

[12] John S. Dzienkowsk, *Ethical Decisionmaking and the Design of Rules of Ethics*, 42 HOFSTRA L. REV. 55, 70-71 (2013) (citing, e.g., Joan C. Rogers, *Ethics 20/20 Commission Airs Proposals on Conflicts-Checking, Choice of Rules Pacts*, BLOOMBERG BNA (Sept. 14, 2011), http://www.bna.com/ethics-2020-commission-n12884903471 (discussing an interview with Anthony E. Davis, Esq. about the limited scope of the Ethics 20/20 Commission's recommendations)) (discussing, for instance, the inability of the ABA to effectively revise the Model Rules to keep current with the realities of modern practice and the debilitating politics within the ABA).

[13] The ABA commenced a review of the Model Rules in 1997 when it established the ABA Commission on Evaluation of the Rules of Professional Conduct ("Ethics 2000 Commission") to consider changes necessary based on developments since the Model Rules were adopted in 1983. For a more detailed description of how changes to the Model Rules can be initiated and adopted, and the history of such amendments, see Dzienkowsk, *supra* note 12, at 87-88. The product of the 20/20 Commission was thoughtfully criticized by Professor Dzienkowsk. *Id.* at 71 ("Most observers viewed Ethics 20/20 as a major opportunity to examine and consider changes that recently have taken place in the legal professions of the United States and other countries. The resulting work product, however, has disappointed many scholars and lawyers because the results do not match the promises.").

Model Rule 1.1.[14] The Comment offers only the following vague and insubstantial advice: "[A] lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology"[15] In terms of other forms of direction, the ABA has only begun to scratch the surface with an opinion letter on social media, but it is directed only at judges.[16] Commentators widely criticized the failure to realistically address technology; for instance, one quipped, "The Deafening Silence of the ABA Model Rules."[17]

Even in an ideal world, the process of the ABA adopting changes to the Model Rules, and urging each bar association to adopt the changes, is political, cumbersome, and lengthy.[18] A level of care to involve all constituencies and give changes long term thoughtfulness may be necessary for crafting a uniform set of rules that lead directly to enforceable punishments,[19] but the ABA has used these procedures to avoid taking action. Expecting timely revisions of the Model Rules

---

[14] MODEL RULES OF PROF'L CONDUCT r. 1.1 cmt. 8 (AM. BAR ASS'N 2013) ("To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.").

[15] *Id.*

[16] ABA Comm. on Prof'l Ethics & Prof'l Responsibility, Formal Op. 13-462 (2013), http://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/formal_opinion_462.authcheckdam.pdf [hereinafter ABA Formal Op. 462] (discussing judge's use of electronic social networking media).

[17] Saleel V. Sabnis, *Attorney Ethics in the Age of Social Media*, June 8, 2016, http://apps.americanbar.org/litigation/committees/professional/articles/spring2016-0616-attorney-ethics-age-social-media.html. He continued, saying

> When the ABA amended the Model Rules of Professional Conduct in 2013, there was no specific mention of social media other than a not-so-subtle reminder that an attorney must stay abreast of changes in technology. The ABA's silence was incongruous with the everyday demands placed on litigators to harvest information on social media.

Id.

[18] *See, e.g.*, Lorelei Laird, *Discrimination and Harassment Will be Legal Ethics Violations Under ABA Model Rule*, A.B.A. J. (Aug. 8, 2016, 6:36 PM CDT), http://www.abajournal.com/news/article/house_of_delegates_strongly_agrees_to_rule_making_discrimination_and_harass/?utm_source=maestro&utm_medium=email&utm_campaign=weekly_email (discussing how difficult it is to amend the Model Rules).

[19] Albeit in a different context, one author's argument that we should not address advances in technology by changing the Rules is convincing. In arguing that the rules of civil procedure should not be amended to take into consideration advances in technology, the author states, "'a change devised now might be irrelevant, and might even be harmful, four years from now.'" Steven S. Gensler, *Special Rules for Social Media Discovery?*, 65 ARK. L. REV. 7, 36 (2012).

to further address technology is at best a long-term goal. In fact, Professor Dzienkowsk argues that "the structure of the ABA is such that few, if any, fundamental reforms have any chance of adoption by the ABA House of Delegates."[20]

B. Professionalism and Civility Standards or Creeds

In an attempt to address the lapses of the Model Rules,[21] many states and courts adopted express statements of acceptable and unacceptable behavior norms.[22] Taking on many different names, these statements of professionalism were originally envisioned to serve an aspirational purpose, clarifying and in some instances going beyond the Model Rules. These published best practices are denominated as professionalism and civility standards, creeds, pillars, codes, etc.[23] I use these common titles interchangeably. The stated expectations in creeds generally aim higher than the minimums delineated in the Model Rules and are designed "to encourage dedication to professionalism and civility."[24] Today, many jurisdictions have taken steps towards making professionalism creeds enforceable.[25]

---

[20] *Id.* at 92.
[21] *Id.* at 73 (nothing that codes of civility "were largely viewed as a solution to the failures of the ABA Model Codes").
[22] A. Darby Dickerson, *The Law and Ethics of Civil Depositions*, 57 MD. L. REV. 273, 302 (1998) (citing 2 GEOFFREY C. HAZARD, JR. & W. WILLIAM HODES, THE LAW OF LAWYERING: A HANDBOOK ON THE MODEL RULES OF PROFESSIONAL CONDUCT § AP4:107, at 1269–70 (2d ed. 1994 & Supp. 1997)) ("Many civility or conduct codes were formulated in the 1980s and 1990s."). The number of creeds seems to have fluctuated over the years from 100 in 1995 to 150 in 2005. Marvin E. Aspen, *A Response to the Civility Naysayers*, 28 STETSON L. REV. 253, 253 n.2 (1998); Allen K. Harris, *Increasing Ethics, Professionalism and Civility: Key to Preserving the American Common Law and Adversarial Systems*, 2005 Prof. Law. 91, 112 (2008) ("More than 150 state, county and city bar associations have adopted professionalism codes to encourage enhanced professional behavior and support increased judicial control of incivility and other unprofessional behavior."). Today there are about 125 such creeds that various organizations and jurisdictions in the United States have adopted. This decline may reflect consolidation, for instance, where lower courts exchange individual creeds for those of the state or circuit. The ABA has compiled an extensive, but not exhaustive nor current, list of the professionalism creeds adopted in various jurisdictions around the United States. *Professionalism Codes*, AM. B. ASS'N, http://www.americanbar.org/groups/professional_responsibility/resources/professionalism/professionalism_codes.html (last updated Aug. 2012).
[23] For a list of extant creeds and how they are styled, see Preston & Lawrence, *supra* note 11, at app. A.
[24] *Id.* at 707.
[25] *Id.*

In professionalism standards, an ideal place to address new and changing issues, there is virtually no treatment of technology abuses.[26] The first two states to hint at the issue in professionalism standards are Utah and Florida.[27] The preamble to Utah Standards of Professionalism and Civility now states:

> Lawyers should educate themselves on the potential impact of using digital communications and social media, including the possibility that communications intended to be private may be republished or misused. Lawyers should understand that digital communications in some circumstances may have a widespread and lasting impact on their clients, themselves, other lawyers, and the judicial system.[28]

The Florida Expectations of Professionalism was amended in 2015 to include:

> 2.5 A lawyer's communications in connection with the practice of law, including communications on social media, must not disparage another's character or competence or be used to inappropriately influence or contact others. (See R. Regulating Fla. Bar 4-8.4(d)).
>
> 2.6 A lawyer should use formal letters or e-mails for legal correspondence and should not use text messages to correspond with a client or opposing counsel unless mutually agreed.[29]

---

[26] Preston & Lawrence, *supra* note 11, at tbl.9. Only three creeds from that survey mention technology in any form, and they address it only in terms of transmitting material. *Id.* The most comprehensive treatment of technology is from the Denver Bar Association:

> 1. We will use data-transmission technologies only as an efficient means of communication and not as a means of obtaining an unfair advantage. The use of such technologies does not require receiving counsel to discontinue other matters to respond.
> 2. We will honor reasonable requests to retransmit materials or to provide hard copies.

Denver Bar Ass'n, *Principles of Professionalism*, DENVER B. ASS'N (May 2007), http://www.denbar.org/repository/Inside_Bar/Professionalism/Professionalism.pdf.

[27] No professionalism statements included other uses of technology as of 2014. *See* Preston & Lawrence, *supra* note 11, at 714 n.75.

[28] UTAH STANDARDS OF PROFESSIONALISM & CIVILITY, pmbl. (2014).

[29] Fla. Bar, *Professional Expectations, 2.5 and 2.6*, FLA. B. 2 (2015), https://www.floridabar.org/TFB/TFBResources.nsf/Attachments/1ACF11084FDADAA285257DE7006B5511/$FILE/Professionalism%20Expectations.pdf?OpenElement. *See also* Fla. Bar, *Oath of Admission to the Florida Bar*, FLA. B. (June 25, 2013), http://www.floridabar.org/tfb/TFBProfess.nsf/basic˘ıew/04E9EB581538255A85256B2F006CCD D?OpenDocument ("To opposing parties and their counsel, I pledge fairness, integrity, and civility, not only in court, but also in all written and oral communications.").

To avoid negligent and accidental abuses, lawyers must be educated in, and then reminded of, the ethical and professional risks.[30] Professionalism creeds, even if not directly enforced, can form a basis for educating and mentoring lawyers with respect to advances in technology.[31] They may be the most appropriate medium for addressing technology issues in the short run until the ABA or another regulator can provide a firmer solution.

C. Ethics Opinions and Court Opinions

Another method of regulating attorney conduct is through the issuance of ethics opinions, which address a question submitted about a specific issue or behavior. In addition, bar associations can issue individualized, ad hoc responses to members of the bar who ask specific questions about the interpretation of the Model Rules. Although some formal opinions include excellent discussion of the risks and expectations, only a very few have addressed technology.[32] The best effort emerged in November 2016 from the District of Columbia Bar Association.[33] But formal opinions are, in practice, of limited use in disseminating widespread standards and guiding future conduct.[34] Few lawyers think to consult ethics opinions on new questions of technology use. Fewer take the time to search through ethics opinions unless they understand they are taking a considerable risk.

[30] MODEL RULES OF PROF'L CONDUCT pmbl. (AM. BAR. ASS'N 1983) (asserting that lawyers must be subject to the profession's rules of conduct as well as their "personal conscience *and* the approbation of professional peers").
[31] Preston & Lawrence, *supra* note 11, at 724.
[32] *See, e.g.*, N.Y.C. Bar Comm. on Ethics & Prof'l Responsibility, Formal Op. 2012-02 (2012), http://www.nycbar.org/ethics/ethics-opinions-local/2012opinions/1479-formal-opinion-2012-02 (last visited Feb. 28, 2015); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 466 (2014); Pa. Bar Ass'n Comm. on Ethics and Prof'l Responsibility, Formal Op. 2014-300 (2014), https://www.pabar.org/members/catalogs/Ethics%20Opinions/formal/F2014-300.pdf.
[33] *See* D.C. Bar Ass'n, Ethics Op. 370: Social Media I: Marketing and Personal Use, https://www.dcbar.org/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm, and D.C. Bar Ass'n Ethics Opinion 371: Social Media II: Use of Social Media in Providing Legal Services, https://www.dcbar.org/bar-resources/legal-ethics/opinions/Ethics-Opinion-371.cfm (last visited Aug. 11, 2017).
[34] Preston & Lawrence, *supra* note 11, at 724.

In addition to ethic opinions, in a few jurisdictions, technology abuses by lawyers have resulted in published opinions by the disciplinary body or the courts.[35] These are useful in training lawyers in this area but tend to involve only the most egregious cases with the most extreme facts. The few precedents on proper technology use are not available in each jurisdiction and are not uniform or consistent in coverage or result.

D. Best Approach for an Immediate Need

Although changes to the Model Rules to account for technology are necessary, the professionalism creeds offer a mechanism that can be more responsive and flexible in the meantime. The potential of stated standards in creeds to address ongoing developments in practice such as the advent of technology is enormous, but the standards are not currently effective. The use of creeds in this function will require focused attention and significant redrafting.[36] Unfortunately, as presently written, almost all of the professionalism creeds are inconsistent, erratic in coverage, and poorly worded. Even the best of creeds are also largely impotent. Including references to common technology related abuses would be an important improvement, but bar associations should also consider using this opportunity for change to

[35] *See, e.g.*, *In re* Eisenstein, 485 S.W.3d 759, 761 (Mo. 2016) (en banc); In re Reines, 771 F.3d 1326 (2014); *In re* Sarah Peterson Herr, Final Hearing Report (Jan. 13, 2014), http://www.kscourts.org/pdf/Herr-Admonition-Final-Report.pdf; *In re* Tsamis, No. 2013PR00095 (Ill. Att'y Registration and Disciplinary Comm'n Jan. 15, 2014), http://www.iardc.org/HB_RB_Disp_Html.asp?id=11221; Missouri v. Polk, 415 S.W.3d 692, 695 (Mo. App. E.D. 2013); *In re* Anonymous Member of S.C. Bar, 709 S.E.2d 633 (2011); *In re* Disciplinary Proceedings Against Beatse, 722 N.W.2d 385, 386–90 (Wis. 2006).

[36] *See, e.g.*, Preston & Lawrence *supra* note 11, at 723.

> The provision that appears most frequently in [various state creeds] is the vague charge to "treat others in a courteous and dignified manner" or to "act in a civil manner," which forty-five of the forty-seven creeds included. This general objective is not very helpful without being further refined and defined within the creed. . . . Also common are provisions urging honesty (without specific definition or elaboration) and provisions against knowingly deceiving or misrepresenting fact or law. Because Model Rules 3.3, 4.1 and 7.1 cover misrepresentation, restating the honesty requirement in unenforceable creeds may suggest that honesty is aspirational, not essential. Such a creed would be more helpful if it articulated borderline cases where the honesty implications are less obviously addressed in the Model Rules.

Id.

undertake a general revision of the wording of their creed and consider options to give them teeth. The survey in *Incentivizing Lawyers to Play Nice: A National Survey of Civility Standards and Options for Enforcement* offers a comparison of the subjects handled in these creeds and commentary on the problems in which some of them wallow. With this information available, each bar association has some comparables to assist them in being more inclusive in the subjects addressed and in improving wording. The ideal would be carefully worded sets of standards that are fairly uniform across the nation.

A related issue is how to make revised creeds more effective in sending the message. Some bar associations are already treating creeds as enforceable in various ways, and others are active in making such creeds effective starting points for lawyer education and guidance.[37] For example, some states are incorporating the creeds into their attorneys' oath; other jurisdictions have implemented programs for referring offenders to investigation boards.[38] Some courts have gone so far as to issue serious sanctions for uncivil conduct violating professionalism creeds.[39] Because of poor drafting and little enforcement, codes of professionalism have failed.[40]

Despite their flaws, professionalism standards offer the best vehicle within the current regulatory framework for meeting the urgent need to address the issue of technology and social media until we can treat these issues more formally in the Model Rules.

E. Speech and Other Legal Implications of Lawyer Regulation

Finally, a note on the speech implications of regulating professionalism and civility is in order. A robust and thorough discussion of the historical and current treatment of the intersection between attorneys and free speech is well beyond the scope of this paper. This issue has been

[37] Preston & Lawrence, *supra* note 11, at 724.
[38] *Id.* at 729-32.
[39] *Id.* at 732-34.
[40] Dzienkowsk, *supra* note 12, at 73.

addressed in detail in a plethora of books and articles.[41] I include here only a short summary of the status of speech and lawyer regulation law in hopes of exposing the implausibility of successful First Amendment challenges to the proposed professionalism creeds.

It is well accepted that licensed members of bar associations are subject to speech restrictions that would not apply to lay persons.[42] These restrictions go well beyond what can be said in court filings, at hearings, and other official contexts and cover speech technically outside of legal system processes.[43] Although this juxtaposition is not without strain, "important state interests compete with attorneys' First Amendment rights and justify greater restrictions on lawyers' speech rights."[44] The Model Rules and local rules of states and courts often restrict and penalize attorneys for what they say. These restrictions generally fall into two broad categories: restrictions on commercial speech[45] and restrictions on speech that affects the administration of

[41] *See, e.g.*, Peter Margulies, *Advocacy as A Race to the Bottom: Rethinking Limits on Lawyers' Free Speech*, 43 U. MEM. L. REV. 319 (2012); Margaret Tarkington, *The Truth Be Damned: The First Amendment, Attorney Speech, and Judicial Reputation*, 97 GEO. L.J. 1567 (2009); Terri R. Day, *Speak No Evil: Legal Ethics v. the First Amendment*, 32 J. LEGAL PROF. 161 (2008); Sarah DeFrain, Note, Grievance Administrator v. Fieger*: The Tenuous Link Between Attorney Silence and Public Confidence in the Legal System*, 54 WAYNE L. REV. 1823, 1824 (2008); W. Bradley Wendel, *Free Speech for Lawyers*, 28 HASTINGS CONST. L.Q. 305 (2001); Kathleen M. Sullivan, *The Intersection of Free Speech and the Legal Profession: Constraints on Lawyers' First Amendment Rights*, 67 FORDHAM L. REV. 569, 569 (1998); Erwin Chemerinsky, *Silence Is Not Golden: Protecting Lawyer Speech Under the First Amendment*, 47 EMORY L.J. 859 (1998).

[42] *In re* Sawyer, 360 U.S. 622, 647 (1959) ("Obedience to ethical precepts may require abstention from what in other circumstances might be constitutionally protected speech."); Sullivan, *supra* note 41, at 569.

[43] *See, e.g.*, Grievance Administrator v. Fieger, 719 N.W.2d 123, 142 (Mich. 2006) (punishing an attorney for undignified speech made on a radio broadcast); *In re* Anonymous Member of S.C. Bar, 709 S.E.2d 633 (2011) (upholding reprimand of attorney for email communication made to opposing counsel outside of formal proceedings).

[44] Day, *supra* note 41, at 162 (citations omitted); *see In re* Snyder, 472 U.S. 634, 644 (1985) ("'Membership in the bar is a privilege burdened with conditions.' [An attorney is] received into that ancient fellowship for something more than private gain. He [becomes] an officer of the court, and, like the court itself, an instrument or agency to advance the ends of justice.") (alterations in original); *Grievance Administrator*, 719 N.W.2d at 142 (holding that coarse attorney speech "warrants no First Amendment protection when balanced against the state's compelling interest in maintaining public respect for the integrity of the legal process") (citing United States v. O'Brien, 391 U.S. 367, 377 (1968)).

[45] *E.g.*, MODEL RULES OF PROF'L CONDUCT r. 7.1 (AM. BAR ASS'N 2013); SUPREME COURT OF OHIO COMM'N ON PROFESSIONALISM, PROFESSIONAL IDEALS FOR OHIO LAWYERS AND JUDGES (2013), https://www.supremecourt.ohio.gov/Publications/AttySvcs/proIdeals.pdf.

justice.[46] In deciding whether a restriction is constitutionally permissible, the court weighs "the State's interest in regulation . . . against a lawyer's First Amendment interest in the kind of speech that [is] at issue."[47] Where the restriction is supported by a compelling governmental interest, it will be upheld as constitutional.[48] In general, the state's interest in regulating commercial speech is less compelling than the interest in regulating attorney speech that affects the administration of justice.[49] It follows, then, that rules restricting attorney commercial speech are sometimes invalidated when challenged on First Amendment grounds, whereas rules implicating the administration of justice and the image of the profession—such as the majority of the professionalism creeds herein discussed—are generally upheld as constitutional.[50] Attorneys knowingly and willingly enter into a highly regulated profession, implicitly waiving the right to unrestrained expression.[51] They should expect to be subjected to some speech restrictions by virtue of being "officers of the court," capable of influencing the administration of justice.[52]

In conclusion, regulation of attorney conduct is generally allowed even when it involves speech. Many provisions of the Model Rules address restrictions on speech. The suggestions in this Article for clarifying and modifying creeds of professionalism, in the short term, and the

---

[46] *E.g.*, MODEL RULES OF PROF'L CONDUCT r. 3.6 (AM. BAR ASS'N 2013); WASH. STATE BAR ASS'N, CREED OF PROFESSIONALISM (2001), http://www.wsba.org/Legal-Community/Committees-Boards-and-Other-Groups/Professionalism-Committee/~/media/Files/Legal%20Community/Committees_Boards_Panels/Professionalism%20Committee/Creed%20of%20Professionalism.ashx.

[47] Gentile v. State Bar of Nevada, 501 U.S. 1030, 1073 (1991).

[48] *See* cases cited *supra* note 44 (describing what constitutes a compelling government interest).

[49] *See* Kyle Lawrence Perkins, *Attorney Advertising: The Marketing of Legal Services in the Twenty-First Century*, 35 GONZ. L. REV. 99 (2000).

[50] *E.g.*, Zauderer v. Office of Disciplinary Counsel of Supreme Court of Ohio, 471 U.S. 626 (1985) (nullifying a state ban on the use of pictures in legal advertisements); *In re* Snyder, 472 U.S. 634 (1985) (reversing an attorney's suspension for heated criticism of the judiciary's administration of the Criminal Justice Act); Bates v. State Bar of Arizona, 433 U.S. 350 (1977) (striking Arizona's flat ban on attorney advertising of legal services, but leaving open other options to regulate advertising attorneys); *cf.* cases cited in *supra* note 44 (upholding restrictions on attorney speech); *see also* Mattei Radu, *The Difficult Task of Model Rule of Professional Conduct 3.6: Balancing the Free Speech Rights of Lawyers, the Sixth Amendment Rights of Criminal Defendants, and Society's Right to the Fair Administration of Justice*, 29 CAMPBELL L. REV. 497 (2007) (arguing that Rule 3.6 strikes an appropriate balance between an attorney's right to free speech and the states' valid interest in the proper administration of justice).

[51] *See* DeFrain, *supra* note 41.

[52] *Id*. at 1844.

Model Rules, in the long term, are well within the exceptions for regulating lawyers.

II. WHY TECHNOLOGY ABUSES WARRANT IMMEDIATE AND TARGETED COVERAGE

Technology use imposes both unique and heightened risks to lawyers, clients, and the legal system. As compared to the type of conduct that was originally targeted in the Model Rules and professionalism creeds, the features of electronic communications make more likely unethical and unprofessional behavior and, when it occurs, more damaging to individuals and the legal system.[53] The interests and values that animate the Model Rules and creeds are the same whether on or offline. But the ways the harm is inflicted is subtler and outside of the awareness of many attorneys, even those who are not naïve or inexperienced in the capacities of technologically. Thus, a tantrum online is much more likely to be exposed and disseminated than oral conversations or a sheet of paper. The digital era represents some fundamental behavioral and attitudinal changes.

> With social media, the world is literally just a few mouse clicks away from a company's most confidential information, raising growing concerns about a company's own employees disclosing confidential information via social media. Exacerbating this is the fear that social media has desensitized people to the fact of disclosure of formerly private information because so much of it is done voluntarily - and so easily. When taken with the tendency of social media users—especially younger ones—to blur the line between social life online and work, crucial proprietary information can be out the door almost before the employee knows it. The concept of information—any information—being private is almost obsolete to many people. If they have access to it, what's so bad about others having it?[54]

This Part II reviews various non-exclusive reasons why technology warrants specific attention in the regulation of the profession.

[53] *See, e.g.*, Catherine J. Lanctot, *Becoming A Competent 21st Century Legal Ethics Professor: Everything You Always Wanted to Know About Technology (but Were Afraid to Ask)*, 2015 PROF. LAW. 75, 91–95 (2015) (citing State Bar of Cal. Standing Comm. on Prof'l Responsibility & Conduct, Formal Op. 2010-179 (2010)).
[54] Michael C. Smith, *Social Media Update*, 58 THE ADVOC. (TEXAS) 2, 4 (2012).

A. Lack of Anonymity and Privacy

The internet creates an unwarranted illusion of anonymity and privacy. Although an expert in encryption, Tor, and anti-trace relays can hide the source and content of some messages, the average internet user cannot expect privacy or anonymity unless no one is trying to find or unmask a post. Any savvy computer user can trace the source IP address for a post and the identifying MAC number of the originating computer. In addition, many lawyers are still extremely sloppy about creating secure and uncommon passwords and then keeping the passwords private.[55] Leaving a confidential letter or an ill-advised note on one's desk or within easy access of a determined snooper is unwise. Stepping away from a computer that is logged into a user's account runs the risk of exposing what is on the screen, and anything else a search of the computer or a look at browsing history might reveal.

Federal laws cover the intentional interception of electronic transmissions and hacking or exceeding access authorization. [56] Additionally, unauthorized access to electronic information is covered in some states by the common law trespass to chattels.[57] However, these laws have not prevented wide scale violations by people unaware of the law, the risk of being caught, and the seriousness of the implications. Furthermore, in most cases, even when a perpetrator is caught, the harm has already been done. Once an embarrassing or unethical communication has been

---

55

> Using the same password for all password-protected services you use means that when someone obtains your password for one of these sites, they will have access to all of them. Using words from the dictionary for a password means a brute force dictionary attack by hackers will crack your password. Using long strings of letters and symbols and numbers means that passwords will be difficult to remember. Many sites now require the use of numbers and characters in passwords.
>
> It is time to start using a password manager. . . . A password that is short and simple enough for you to remember is too short and simple to be secure.

Jim Calloway, *Client Confidentiality, Personal Privacy, and Digital Security*, OKLA. BAR J., Vol. 87, Dec. 17, 2016, http://www.okbar.org/members/MAP/MAPArticles/HotPracticeTips/ClientConfidentialityPersonalPrivacy.aspx (last visited July 31, 2017). For examples of password problems involving lawyers, see notes 140-43, 152, 159, 193 *infra*.

56 *See, e.g.*, 18 U.S.C. § 2703 (2009).

57 *See, e.g.*, Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 404 (2d Cir. 2004).

made public, arguing that access to internet posts was obtained illegally is not an effective response.[58] As in the case of *Yath v. Fairview Clinics*, once the information about plaintiff's sexually transmitted disease and her new lover had travelled through her husband's family and onto Myspace.com, it was little comfort that the information had been obtained illegally by an employee of a medical clinic.[59]

Moreover, the law does not prevent the reproduction and distribution of information by a third-party who did not participate in the illegal access. In *Bartnicki v. Vopper*, an activist allegedly found a tape of a private cell phone conversation in his mailbox, which he then sent to the press.[60] Because it could not be proved that the recipient of the tape was a party to the illegal acquisition of the conversation, the wiretap statutes do not apply and spreading this information was legal.[61]

B. Rights Waivers

Increasingly, Internet users are waiving what rights to privacy and protection they have. Websites often assert a "terms of use" policy, "end user license agreement," or the like in clickwrap or even browsewrap form.[62] These wrap contracts may give the website owners or operators a license to use customer postings and photographs for their own purposes and to sell or sublicense these to others.[63] If so, the author and original copyright owner of the post cannot force the site, or the assignees and sublicensees, to take it down.[64] Some websites offer processes

[58] Ask Sarah Pallin and Judge Kozinsky of the Ninth Circuit.
[59] Yath v. Fairview Clinics, N.P., 767 N.W.2d 34, 38-40 (Minn. Ct. App. 2009).
[60] Bartnicki v. Vopper, 532 U.S. 514, 519 (2001).
[61] *Id.*
[62] Cheryl B. Preston & Eli W. McCann, *Unwrapping Shrinkwraps, Clickwraps, and Browsewraps: How the Law Went Wrong from Horse Traders to the Law of the Horse*, 26 BYU J. PUB. L. 1, 19-22 (2011).
[63] For example, Facebook's terms of service provide that "you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook." *Statement of Rights and Responsibilities*, FACEBOOK, https://www.facebook.com/legal/terms (last revised Jan. 30, 2015).
[64] Venkat Balasubramani, *Xcentric Ventures Chips Away at Small Justice's Copyright Workaround to Section 230*, TECH. & MARKETING L. BLOG (April 5, 2014), http://blog.ericgoldman.org/archives/2014/04/xcentric-ventures-

that allow users to erase personal information themselves; however, this is not a guarantee of privacy and creates no legal obligation for the service provider.[65]

Courts have upheld the right of employers to access the content of internet transmissions and stored computer content originating from, received on, or saved on company owned machines. The same applies to employer owned internet access accounts and mobile devices.[66] Some employers disclose their right to such access and require employees to consent in an internet use policy or employee handbook. Others do not, but courts have generally found that an employee cannot have a reasonable expectation of privacy in such content.[67]

C. Misplaced Trust

Many communicants on the internet share an unfounded belief that their message will be seen only by the intended recipients. Recently, the adultery-based dating website Ashley Madison suffered a serious hack that exposed the names and email addresses of the site's users, which information went viral.[68] As with prior, well publicized disclosures, these hackers will inspire copycats.[69] Any promise that digital information will be hermetically sealed in a mayonnaise jar is tenuous. Although secrets have always spread, in years past fewer people had the technology to rapidly share secrets. Moreover, passed-on oral information was recognized to become increasingly less reliable with each subsequent retelling while exact copies of a writing

---

chips-away-at-small-justices-copyright-workaround-to-section-230.htm (saying that even though a lawyer gained copyright to the contents of a website post, that website had a right to keep the post online because of the license granted in the terms of service).

[65] *Statement of Rights and Responsibilities*, FACEBOOK, https://www.facebook.com/legal/terms (last revised Jan. 30, 2015) ("When you delete [intellectual property] content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others).").

[66] *See, e.g.*, Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (holding as early as 1996 that there is "no reasonable expectation of privacy in e-mail communications voluntarily made by an employee over the company e-mail system, notwithstanding any assurances that such communications would not be intercepted by management.")

[67] *Id.*

[68] Jeff Yang, *Ashley Madison Hack: Privacy Becomes Extinct*, CNN (Aug. 27, 2015), http://www.cnn.com/2015/08/27/opinions/yang-ashley-madison-hack/.

[69] *Id.*

or a tape are hard to refute.

Even if no one intercepts an online conversation or circumvents privacy settings, the content of group posts is only as trustworthy as the others who have authorized access. Friends, family members, coworkers, and others may not understand that another's posts made in a "private" group should not be copied and sent to outsiders.[70] This often happens without the slightest intent to criticize or harm the author, but some later recipient may have other ideas. One MySpace user posted a journal entry that was later submitted to a local newspaper. [71] The court reached the obvious holding on the law: users of social media have no reasonable expectation of privacy.[72] In a Fourth Amendment context, one court observed: "While [the user] undoubtedly believed that his Facebook profile would not be shared with law enforcement, he had no justifiable expectation that his 'friends' would keep his profile private."[73]

The ABA's formal opinion on social media issued to judges states what every lawyer should be taught: "[Lawyers] must assume that comments posted to [a social media site] will not remain within the circle of the [lawyer's] connections. Comments, images, or profile information . . . may be electronically transmitted without the [lawyer's] knowledge or permission to . . . unintended recipients."

In addition, an array of observers may be present in a chatroom without disclosing their presence or their real identity. Interested third parties may convince another member of the group to disclose his or her password, and access the computer of a co-worker or family member while it is logged into a chat room, blog, or social media site. In the opinion regarding proper

[70] ABA Formal Op. 462, *supra* note 16 ("Judges must assume that comments posted to [a social media site] will not remain within the circle of the judge's connections. Comments, images, or profile information . . . may be electronically transmitted without the judge's knowledge or permission to persons unknown to the judge or to other unintended recipients.").
[71] Moreno v. Hanford Sentinel, Inc., 172 Cal. App. 4th 1125, 1130 (2009).
[72] Moreno v. Hanford Sentinel, Inc., 172 Cal. App. 4th at 1130.
[73] United States v. Meregildo, 883 F. Supp. 2d 523, 526 (S.D.N.Y. 2012) (citations omitted).

technology use for judges, the ABA formal opinion correctly observed a truth applicable to all technology users:

> In contrast to fluid, face-to-face conversation that usually remains among the participants, messages, videos, or photographs posted to social media may be disseminated to thousands of people without the consent or knowledge of the original poster. Judges must assume that comments posted to an ESM site will not remain within the circle of the judge's connections. Comments, images, or profile information . . . may be electronically transmitted without the judge's knowledge or permission to persons unknown to the judge or to other unintended recipients.[74]

D. Ubiquity and Diffusion

Internet use has become pervasive in all ages and groups, including lawyers.[75] Every person can be a publisher on a national and global scale with a few keystrokes and a click. Each person's associates, friends, and relatives (including prior acquaintances entirely ignored for the last forty years), are now sending numerous messages that seem to warrant a quick reply. The ease and speed of electronic communications means writers give less thought to what they tweet back.[76] Conversations in which two like-minded people whispered casually at the watering hole after work are now taking place online and can, in painful detail, be displayed in writing and out of context for the world to see. Unprofessional and hotheaded comments posted online are prone to being found, copied, reposted, and forwarded to the person berated in a way that face-to-face comments between two people would not. The risk that maladroit messages will be forwarded to a judge, opposing counsel, client, juror or other target is vastly magnified. Thus, electronic communications are more lethal than prior modes of discussion.

---

[74] ABA Formal Op. 462, *supra* note 16, at 2.

[75] *See* Allison Shields, *Blogging and Social Media*, ABA TECHREPORT 2016, https://www.americanbar.org/groups/law_practice/publications/techreport/2016/social_media_blogging.html (last visited Aug 11, 2017) (reporting that "76% of respondents report that they individually use or maintain a presence in one or more social networks for professional purposes. This number has also remained relatively steady since 2013. Not surprisingly, the group most likely to report individually using or maintaining a presence in a social network is respondents under the age of 40, at 88%, followed by those between the ages of 40-49 at 85%, then 50-59 years old at 81%, and 64% of those 60+ years old, again all remaining reasonably consistent from 2013 to the present.").

[76] Given the nature of some of President Trump's tweets, hopefully they were not thoroughly thought through.

E. Verifiability

The accuracy of a report of others' statements using electronic communication can be easily verified, whereas oral interactions cannot. It is difficult to "spin" the meaning when the exact words used are on display. The experience of Federal District Judge Cebull serves as a prime example.[77] After he forwarded a racially charged email to some "old buddies," the exact content of that email was forwarded in a chain to unintended recipients.[78] Judge Cebull lamented, "It was not intended by me in any way to become public."[79] Unfortunately for the judge, his name was attached to contents circulated beyond his reach.

F. Permanence and Aggregation

The internet's memory cannot be controlled by the original poster.[80] A computer drive or disk can keep innumerable messages without bothering with space, filing cabinets, or document clerks. And unlike oral or print communication, digital information is easily searchable by names and other terms. A tidbit of a client confidence in a tweet can be connected to other bits of digital information to reveal information lawyers believe was never told to anyone. Internet service providers often cache copies of "deleted" data forever.[81] Material thought to have been destroyed can resurface at a later date.[82] In contrast to the European Union,[83] the United States does not

[77] Kim Murphey, *Montana Judge Admits Sending Racist Email About Obama*, L.A. TIMES (Feb. 29, 2012), http://articles.latimes.com/2012/feb/29/news/la-montana-judge-admits-sending-racist-email-about-obama-20120229.
[78] *Id.*
[79] *Id.*
[80] Jeffrey Rosen, *The Web Means the End of Forgetting*, N.Y. TIMES (July 21, 2010), http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all&_r=0.
[81] *What Is Browser Caching and ISP Caching?* Geek Host, https://geekhost.ca/supp/knowledgebase.php?action=displayarticle&id=90 (last visited July 31, 2017)
[82] ABA Formal Op. 462, *supra* note 16 ("Such data [posted to social media] have long, perhaps permanent, digital lives such that statements may be recovered, circulated or printed years after being sent.").
[83] *See, e.g.*, Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 E.C.J. 317; Charles Arthur, *Explaining the 'Right to be Forgotten' – The Newest Cultural Shibboleth*, THE GUARDIAN (May 14, 2014, 1:42 PM EDT), http://www.theguardian.com/technology/2014/may/14/explainer-right-to-be-forgotten-the-newest-cultural-shibboleth; Julia Fioretti, *France Fines Google Over 'Right to Be Forgotten'*, REUTERS (Mar. 24, 2016), http://www.reuters.com/article/us-google-france-privacy-idUSKCN0WQ1WX; Lance Ulanoff, *EU Wants a 'Right*

require internet service providers to delete electronic information unless the content is illegal and the provider is under notice.[84]

G. Instantaneity and Informality

The instantaneity of online communications permits, if not encourages, severely pococurante messages. Because of the ease and informality of online communication, people say things online that they would not say in a letter or face-to-face. [85] Social norms that encourage people to self-regulate—for example, shunning or reprimands from neighbors, family, and coworkers—are largely lost online.[86] Internet use seems to override any sense of inhibition or caution, perhaps because users wrongly harbor an illusion that their communication will never reach beyond the intended recipient. In addition, digital natives are carrying on more and more conversations electronically that historically were not in writing. Given the immediacy of texting coupled with clumsy, tired thumbs, an electronic reply may be more easily misspelled, misstated, and mis-aimed.

---

to Be Forgotten,' But the Internet Never Forgets, MASHABLE (May 13, 2014), http://mashable.com/2014/05/13/eu-google-ruling-op-ed/#wImNGubLpqqW.

[84] David Wolpe, *Drunk Mistakes Posted on Facebook Are Forever*, TIME (Apr. 28, 2015), http://time.com/3838345/drunk-social-media-permanence/.

[85] Elizabeth Bernstein, *Why We Are So Rude Online*, WALL ST. J. (Oct. 2, 2012), http://www.wsj.com/articles/SB10000872396390444592404578030351784405148.

[86]

> Anonymity removes many of the social controls that may have deterred offenders in the pre-Internet era. Anonymity also reduces accountability and accuracy. . . While one may argue that anonymously authored postings are not as credible as identified postings, the mere existence or prevalence of online gossip or online insults may have a negative effect even where such information is refuted or discredited. One study showed that repeated exposure to information made people believe the information was true, even where the information was identified as false. The "illusion of truth" appears to come from increased familiarity with the claim and decreased recollection of the original context in which the information was received.

Nancy S. Kim, *Web Site Proprietorship and Online Harassment*, 2009 UTAH L. REV. 993, 1009.

Significant work has been done on the power to control behavior generated by the social expectations of members of communities and even strangers who share expectations and whose shock or disapproval is enough to discourage unacceptable behavior. *See generally* Cass R. Sunstein, *Social Norms and Social Roles*, 96 COLUM. L. REV. 903 (1996); ROBERT ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES (Harvard Univ. Press 1991); and Lawrence Lessig, *The Regulation of Social Meaning*, 62 U. CHI. L. REV. 943 (1995). For many online posts, anonymity is assured unless someone is motivated enough to expend time and money in uncovering the source. *See* Kim, *supra*.

Language in electronic messages is typically more casual and filled with hyperbole and tasteless attempts at humor. Research by social scientists reveals that we tend to be vastly overconfident in our ability to clearly communicate by email.[87] Comments that might be in an offhand aside to the person in the next seat in a meeting can, and frequently do, implicate flaws in clients, other lawyers, judges, jurors, and the legal system, and project messages that erode public trust in the legal system. When made electronically, such comments can be preserved, verified, and disseminated in writing to a wide audience.

Employees who would not confront a boss in the hall seem willing to say what they think online. An employee shared that she and another employee had been fired on Facebook.[88] A third worker commented on the post, stating that "[the boss] did both of y'all wrong." [89] Word got back to the boss,[90] who disapproved of what could be read as disloyalty. The worker then posted: "[S]omeone did not like what I had to say even though it's MY fb, MY post/comment. I can say what I please. don't like whatcha see? then scoot."[91] The person who had to "scoot" was the worker, who was fired and initially denied unemployment benefits.[92]

The sender may choose the wrong emoji. I once included a face with big tears to convey sadness and the recipient had to tell me that this emoji conveys laughing so hard that one is crying. The message, thus, was inappropriate. Many electronic devices autocorrect words that appear (to it) to be misspelled. The text is replaced with what may be a common-sense choice but

[87] See various studies discussed in Kristen E. Murray, *You Know What I Meant: The Science behind Email and Intent*, forthcoming 14 J. AM. LEGAL WRITING DIRECTORS (2017), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2952519.
[88] Venkat Balasubramani, *Employee Kvetching About Job On Facebook Still Entitled To Unemployment Benefits*, TECH. & MARKETING L. BLOG (Jan 2, 2016), http://blog.ericgoldman.org/archives/2016/01/employee-kvetching-about-job-on-facebook-still-entitled-to-unemployment-benefits.htm.
[89] Balasubramani, *supra* note 88.
[90] *Id.*
[91] *Id.*
[92] *Id.* She was first denied unemployment benefits and consequently sued the company. The court held that Martinez (the third worker) was entitled to benefits. *Id.*

is inaccurate, sometimes after the writer has moved down several lines. My daughter announced the birth of her baby named Hugh. A friend's voice text came across as "Congrats on BBQ." This is a trivial error; others might be significant. Following an interview with a Salt Lake City firm, one applicant wrote to praise the firm for its "nurturing" of new associates and instead praised their "neutering" of new associates.[93]

Often, the author of a post believes that catchy comments will be seen as a harmless jest. However, for defamation purposes, that assumption cannot be relied upon. At least one judge has ruled that comments made on Twitter should be taken just as seriously as comments in other, more formal settings.[94] After Courtney Love tweeted that her former lawyer was "bought off," the lawyer brought a libel suit.[95] Counsel for Courtney Love argued that the tweet was just the hyperbole often found on the internet. The court ruled that Love made the comments with "a widely used internet vehicle for communicating personal views,"[96] and will be held to the words she used.[97] This is only the decision of a single district judge, but the analysis is convincing and other courts may be willing to take online messages literally.[98]

[93] Message on file with author. It is probably true that neutering new associates would result in higher billable hours.
[94] Martha Neil, *Courtney Love Testifies at First US 'Twibel' Trial, Sued by Her ex-Lawyer over Critical Tweet*, A.B.A. J. (Jan. 16, 2014, 3:25 PM CDT), http://www.abajournal.com/news/article/courtney_love_takes_stand_in_former_attorneys_libel_lawsuit_over_critical/.
[95] Bill Hetherman, *Lawsuit Against Courtney Love Can Proceed, Judge Rules*, L.A. DAILY NEWS (Dec. 20, 2013, 6:59 AM PST), http://www.dailynews.com/general-news/20131220/lawsuit-against-courtney-love-can-proceed-judge-rules.
[96] *Id.*
[97] *Id.*
[98] Ellyn Angelotti, *How Courtney Love and U.S.'s First Twitter Libel Trial Could Impact Journalists*, POYNTER (Jan. 14, 2014, 8:00 AM), http://www.poynter.org/latest-news/top-stories/235728/how-courtney-love-and-u-s-s-first-twitter-libel-trial-could-impact-journalists/. This article suggests that "this decision could be influential in future [Twitter-libel] cases" and urges publishers to "keep a close eye on how this court applies traditional defamation to Twitter." *Id.*; *see also* Lizzie Plaugic, *Ciara hits Future with $15 million libel suit over tweets*, THE VERGE (Feb. 9, 2016, 12:40 PM), http://www.theverge.com/2016/2/9/10949564/ciara-future-lawsuit-slander-tweets-interviews.

H. Lack of Context

Internet interactions can be taken easily out of context.[99] Ask Sarah Palin about seeing Russia[100] and Michelle Obama about being proud of her country.[101] It is much easier to copy and paste word snippets that, without context, carry a different meaning than the speaker or poster intended. The casualness and back and forth of an email chain means that writers may be more terse and improvident than in other settings. Without the entire chain, a statement in one email could carry an entirely different meaning.

Internet posts consist only of bare words and an occasional emoji, without the body language usually present in face-to-face conversations and without the tonal distinctions of oral conversations.[102] The impediments in accurately conveying a message electronically are so acute that some have called for punctuation that indicates mood (such as one to denote sarcasm).[103] Facebook even started experimenting with a "satire" tag to help users avoid getting duped by popular satiric news stories.[104]

The speed and the ease with which an electronic communication can be sent means that an errant click on "reply all" could send one's snotty commentary on a post to the entire listserv. Other potential pitfalls lie in the ability to copy and paste a long list of recipients' emails without

---

[99] ABA Formal Op. 462, *supra* note 16 ("[R]elations over the Internet may be more difficult to manage because, devoid of in-person visual or vocal cues, messages may be taken out of context, misinterpreted, or relayed incorrectly.").

[100] Eoin O'Carroll, *Political misquotes: the 10 most famous things never actually said*, CHRISTIAN SCI. MONITOR, June 3, 2011, https://www.csmonitor.com/USA/Politics/2011/0603/Political-misquotes-The-10-most-famous-things-never-actually-said/I-can-see-Russia-from-my-house!-Sarah-Palin.

[101] Cate Carrejo, *The Infamous Comment Michelle Obama Made In 2008 That Would Be Better Understood Today*, Dec. 27, 2016, BUSTLE, https://www.bustle.com/p/the-infamous-comment-michelle-obama-made-in-2008-that-would-be-better-understood-today-26371.

[102] ABA Formal Op. 462, *supra* note 16 ("[R]elations over the Internet may be more difficult to manage because, devoid of in-person visual or vocal cues, messages may be taken out of context, misinterpreted, or relayed incorrectly.").

[103] Erin McKean, *Yeah, Right*, BOS. GLOBE (Feb. 7, 2010), http://www.boston.com/bostonglobe/ideas/articles/2010/02/07/yeah_right/.

[104] Anu Passary, *Facebook Tests 'Satire' Tag to Avoid Confusion on News Feed*, TECH. TIMES (Aug. 17, 2014, 9:33 AM), http://www.techtimes.com/articles/13230/20140817/facebook-tests-satire-tag-to-avoid-confusion-on-news-feed.htm.

reentering or rereading each. A prior message may have been used to reply. The parties believe the new interchange includes only two people, not realizing that the "reply" went to everyone on the list. Just recently, one of my research assistants accidentally sent a "kissy face" image and a personal message to his landlord; it was intended for his wife. No harm done, but it is easy to imagine more damaging images and messages. The old-fashioned process of printing duplicates and typing out the addresses on envelopes, by contrast, makes this kind of unintentional over-distribution so much less likely in non-digital contexts.

In a provoking example, after oral arguments for a case involving the State Bar of Nebraska, the former bar president sent an email to the attorneys who had argued for the bar. He also cc'd the bar's Executive Council, which unfortunately included the Chief Justice as the Supreme Court Liaison. The email congratulated the attorneys for dealing with "ill conceived [sic] and uninformed questions" from the bench.[105] Because the Chief Justice had seen the email, he felt it necessary to reveal it to the other members of the court, as an ex-parte communication.[106] This whole embarrassment was facilitated by the ease of including groups in the recipient field of an email without separately inputting names. Clearly, the internet presents a host of new issues that make ethical and professional faux pas more likely and spread their harm more widely.

III. PROPOSED CHANGES TO ADDRESS TECHNOLOGY ABUSE IN THE LAW

Stopping uncivil and unprofessional behavior by lawyers is the focus of many of the Model Rules and the clear intent of professionalism standards. Most printed court and bar association standards include a generalized and overarching statement, such as this one:

[105] Joe Patrice, *This Is Why You Always Check the Address Field Before Sending an Email*, ABOVE THE L. (Oct. 7 2013, 3:42 PM), http://abovethelaw.com/2013/10/this-is-why-you-always-check-the-address-field-before-sending-an-email/.
[106] *Id.*

"[L]awyers shall treat all other counsel, parties, judges, witnesses, and other participants in all proceedings in a courteous and dignified manner."**[107]** The sentiment is noble, but it does little to incentivize change and less to identify when the line is crossed.

In this part III, I discuss how technology use frequently runs afoul of various principles of ethical and professional behavior. I organize this discussion in the numerical order of the individual Model Rule that is most closely associated with a particular type of abuse. I do not mean to suggest that the problems must now be addressed in terms of the Model Rules. Although enforcement actions could currently take the form of violations of the Model Rules, my main concern is preventing abuses in the future. Thus, I suggest first that these issues be explained in an official statement of expectations or a professionalism creed enacted by each bar association and court. At some point, hopefully, the Model Rules will be reexamined to consider express inclusion of these ethical and professional problems in the text of the Model Rules. I order the discussion in accordance with the format of the Model Rules only for convenience. I begin with issues related to the content of Model Rule 1.1. However, the most important discussion falls at the end in the coverage of Rule 8.

A. Rule 1.1: Competence

Model Rule 1.1 requires "competent representation."[108] The ABA 20/20 Commission took a small step toward acknowledging the importance of technology in the practice when they added a comment to Rule 1.1 stating that "a lawyer should keep abreast of . . . the benefits and risks associated with relevant technology."[109] Many states have adopted this provision,[110] including Alabama, Arizona, Connecticut, Delaware, Kansas, New Mexico, New York,

[107] UTAH STANDARDS OF PROFESSIONALISM & CIVILITY r. 1 (2014). Around nineteen states have adopted a similar standard. Preston & Lawrence *supra* note 11, at tbl.1.
[108] MODEL RULES OF PROF'L CONDUCT r. 1.1 (AM. BAR ASS'N 2013).
[109] *Id.* at cmt. 8.
[110] *See* Ambrogi, *supra* note 1.

Pennsylvania, and Utah.[111] Commendably, Florida went beyond the suggested language of Model Rule 1.1 and not only adopted the language of the Rule, but also took a concrete step toward making sure that Model Rule 1.1 is followed, and not just a good suggestion, by requiring Florida lawyers to "take at least three hours of CLE in an approved technology program as part of the 33 total hours of CLE they must take over a three-year period."[112]

Admonitions of competency are being considered or adopted in various states in a variety of alternative forms. Many courts now encourage or require lawyers to conduct discovery in digital formats. A California Ethics Opinion states that if an attorney lacks the required competence for proper e-discovery, she should "(1) acquire sufficient learning and skill before performance is required; (2) associate with or consult technical consultants or competent counsel; or (3) decline the client representation."[113] A few bar association creeds mention use of technology in discovery and transfer of documents.[114]

As technology becomes more and more pervasive, ignorance of beneficial uses of technology is increasingly unacceptable, and can result in very real consequences for lawyers and their clients. Many have opined that not using technology during legal research may constitute a lack of diligence, because online legal research provides the most up-to-date picture

[111] MODEL RULES OF PROF'L CONDUCT r. 1.1 cmt. 8 (AM. BAR ASS'N 2013) (noting the status of adoption of the change).
[112] Victor Li, *Florida Requires Lawyers to Include Tech in CLE Courses*, A.B.A. J. (Feb. 1, 2017 2:10 AM CST), http://www.abajournal.com/magazine/article/technology_training_cle/?utm_source=maestro&utm_medium=email&utm_campaign=tech_monthly.
[113] The State Bar of Cal. Standing Comm. on Prof'l Responsibility & Conduct, Formal Op. Interim No. 11-0004 (2014), http://www.calbar.ca.gov/Portals/0/documents/publicComment/2014/2014_11-0004ESI03-21-14.pdf.
[114] Fla. Bar, *supra* 25, 2.17 ("A lawyer must ensure that the use of electronic devices does not impair the attorney-client privilege or confidentiality."); Los Angeles Chpt., Ass'n Bus. Trial Lawyers, *Ethics, Professionalism and Civility Guidelines* (2016) http://www.abtl.org/la_guidelines.htm (containing an entire section on electronic discovery); UTAH STANDARDS OF PROFESSIONALISM & CIVILITY, *supra* note 24, 14 cmt ("Lawyers should only use data-transmission technologies as an efficient means of communication and not to obtain a tactical advantage.").

of the law.[115] Further, online fact discovery is likely to reveal important additional information to help build a client's case or assess a client's risk. Failing to use technology to streamline practice and save wasted time could lead to fees a court might find unreasonable.[116]

Although most discussion of technology uses and abuses centers on litigators, transactional lawyers are not immune from technoblunders. The recent District of Columbia bar association ethics opinion warns that lawyers entrusted with fulfilling due diligence for cases involving securities, pending sales and purchases, and regulatory compliance must thoroughly review all social media postings and the situation may "require advice about whether social media postings or use violate statutory or rule-based limits on public statement or marketing."[117] It references limitations on such public statements or guidelines from federal, state, and local agencies. It explicitly notes the Security and Exchange Commission's recent action relating to the risk that social media may be a communication about an initial public offering,[118] and that "[i]nadequatly disclosed interactive internet downloads may constitute unfair or deceptive acts or practices in violation of Section 5(a) of the Federal Trade Commission Act."[119] The Model Rules do not address the risks for transaction lawyers, and neither do the professionalism standards of any state. This specificity is novel to the DC bar Ethics Opinion 371. The ABA goes so far to

[115] Ellie Margolis, *Surfin' Safari-Why Competent Lawyers Should Research on the Web*, 10 YALE J. L. & TECH. 82 (2007) ("Courts routinely emphasize the relative ease and quickness of Shepardizing, particularly with the use of Westlaw or Lexis, implying that failing to perform this simple task is a basic lack of diligence.").
[116] Ivy B. Grey, *Not competent in basic tech? You could be overbilling your clients—and be on shaky ethical ground*, May 15, 2017, http://www.abajournal.com/legalrebels/article/tech_competence_and_ethical_billing ("Failing to become competent in technology would also lead to unreasonable fees. This may be more than a billing write-off—it may constitute an ethical violation.").
[117] D.C. Op. 370, *supra* note 32.
[118] *Id.* (citing Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: Netflix, Inc., and Reed Hastings Exchange Act, Release No. 69279, 105 SEC Docket 4327 (Apr. 2, 2013) (interpreting Commission Guidance on the Use of Company Web Sites, Exchange Act Release No. 58288 (Aug. 7, 2008)) [hereinafter SEC Report]).
[119] DC Op. 371 (citing SEC Report, at 5: "at 5 ("[I]ssuer communications through social media channels require careful Regulation FD analysis comparable to communications through more traditional channels [and] the principles outlined in the 2008 Guidance . . . apply with equal force to corporate disclosures made through social media channels.")).

change the Model Rules to require lawyers to be competent in electronic communications but offers no guidance for transactional lawyers.

Not just disuse, but mistakes in understanding how technology works can have serious consequences. In Wisconsin for example, a lawsuit was recently dismissed because of an email that allegedly landed in a lawyer's junk mail folder.[120] The plaintiff and his lawyer Timothy Davis did not appear at a deposition on June 6th because "the email notice went to the lawyer's junk email folder."[121] Apparently no one in the office noticed a mailed notice. Assuming the lawyer in this case is telling the truth, this example is a warning about relying on the delivery of electronic notices and neglecting careful handling of hard copy mail. In addition, Davis alleges that the lawyers for the opposition did not receive discovery documents he sent because their system could not receive email files larger than ten megabytes.[122] Lawyers must be on the alert for sending documents in smaller batches or emailing opposing counsel to be sure that files were received before assuming they were.

Although a lack a technological savvy may not always result in consequences as drastic as having a case dismissed or missing discovery deadlines, it will never do the client any favors. One way to approach this issue would be to amend the requirements for continuing education to require some credits for classes on properly using technology in the practice of law. In the last year promising materials are starting to be available for even the smallest bar association to use in providing at least initial education to members.[123]

---

[120] Debra Cassens Weiss, *Lawyer says he missed deposition because email notice went to his junk folder*, A.B.A. J. (Jul. 5, 2017, 9:42 AM CDT), http://www.abajournal.com/news/article/lawyer_says_he_missed_deposition_because_email_went_to_his_junk_mail_folder/?utm_source=maestro&utm_medium=email&utm_campaign=weekly_email

[121] *Id.*

[122] *Id.*

[123] *See, e.g.*, Pamela Chandran & Robert C. Nagle, *Attorney Misconduct on Social Media: Recognizing the Danger and Avoiding the Pitfalls*, ABA Section of Labor and Employment Law Committee on the Development of Law under the NLRA Midwinter Meeting (2017),

Unfortunately, much of the education on social media available to lawyers is promotional. That means it is teaching about how to promote yourself and your practice and it is given by commercial interests that are happy to assist you by selling use of their platforms. For instance, Kevin O'Keefe, CEO of LexBlog, introduces his various presentations with this:[124]

> The key for lawyers is learning how to turn the digital dials by using social networks and media effectively. Learning here comes from trial and error.
>
> Adapting to the cultures each social media present is like traveling to a foreign country. You get comfortable over time and keep the faux pas to a minimum as you start.[125]

By encouraging lawyers to dive in and hope to overcome mistakes over time is the wrong message. Lawyers should be taught how to avoid "faux pas" as well as ethical and professional violations first.

While waiting for the Model Rules to be more explicit, bar associations should consider professionalism standards that encourage the use of electronic discovery and recommend online factual research. Moreover, technological competency requires recognizing the risks of online social media and electronic communications. No lawyer is competent to practice law in this century without becoming aware of the risks of electronic communications and social media as described in Part II. A general statement in a professionalism creed could include the following language, but as the following Subparts illustrate, various issues require more detailed individual coverage.

---

http://www.americanbar.org/content/dam/aba/events/labor_law/2017/02/dll/papers/nagle%20chandran.authcheckdam.pdf; ABA, Social Media Basics, On-Demand CLE, Jan. 18, 2017, https://shop.americanbar.org/ebus/store/productdetails.aspx?productId=263192541.

[124] Kevin O'Keefe, Nuts and Bolts of Social Media, LexBlog, http://rlhb.wp.lexblogs.com/wp-content/uploads/sites/111/2014/11/Social-Media-Nuts-and-Bolts-by-Kevin-OKeefe.pdf (last visited Aug. 1, 2017). This material and versions of it are promoted widely. The presentation O'Keefe gave to the Utah Bar Association is available at https://www.utahbar.org/wp-content/uploads/2016/12/Social-Media-Nuts-and-BoltsUtah-Bar-Association.pdf (last visited Aug. 1, 2017), and the slides are available at https://www.slideshare.net/kevinokeefe/utah-bar-association-nuts-and-bolts-of-social-media (last visited Aug. 1, 2017).

[125] *Id.*

> Lawyers should educate themselves on the merits of e-discovery and online research, as well as the obligations of researching social media in the course of due dilligence. Further, lawyers should be aware of potential negative consequences of using digital communications and social media, including the possibility that communications intended to be private may be republished or misused. Lawyers should understand that digital communications in some circumstances may have a widespread and lasting impact on their clients, themselves, other lawyers, and the judicial system.

B. Model Rule 1.6(a) and (c): Confidentiality of Information

Model Rule 1.6(a) provides: "A lawyer shall not reveal information relating to the representation of a client "except under limited circumstances.[126] Of course, attorneys have been on notice about the importance of confidentiality for a century. However, attorneys may not recognize the ways that electronic communications, research, and storage lures a conscientious attorney into inadvertent violations.

What lawyers should be required to know is that, with more options of storing and transmitting client information, inadvertent disclosure of client information is much more likely in the cyberworld.[127] Protection of important digital data is often handled too casually by attorneys. The frequency of online posts, texts, tweets, and other forms of social media correspondingly increase the risk of exposing confidential information. Also, the ease and instantaneity of the medium encourages sloppy and thoughtless disclosures. Something about the internet leads people to overshare, to unduly trust those they imagine are watching, and to fail to use caution or even proofread.[128] Lawyers must be aware that, in addition to their own electronic

---

[126] MODEL RULES OF PROF'L CONDUCT r. 1.6(a) (AM. BAR ASS'N 2014).

[127] *See* Michael E. Lackey, Jr. & Joseph P. Minta, *Lawyers and Social Media: The Legal Ethics of Tweeting, Facebooking and Blogging*, 28 TOURO L. REV. 149, 155–56 (2012) ("The ease of sharing and publicizing information through social media, however, raises a danger that lawyers might fall afoul of this duty [of confidentiality]."); Anne Klinefelter, *When to Research is to Reveal: The Growing Threat to Attorney and Client Confidentiality from Online Tracking*, 16 VA. J.L. & TECH. 1 (2011) (discussing the possibility that third parties can gain access to private information through online tracking).

[128] *E.g.*, Martha Neil, *Lawyer's request for reprimand over her own web comments nixed by top state court*, A.B.A. J. (Mar. 20, 2013, 4:11 PM),

devices, access to confidential information may occur from third parties' devices when they receive or generate messages to the lawyer.

Lawyers fail to consider the various kinds of technoblunders that give rise to ethical and professional risks. This Part reviews common categories of confidentiality breaches arising with the use of technology.

1. Oversharing

Attorneys have been known to complain about their day's work or regale others with tales of competence and success in particular cases or transactions. Some of these communications provide enough information to lead a recipient to figure out exactly what client and what transaction was involved, even if the lawyer did not mention specific names or obvious facts. Historically, these kinds of sloppy and "accidental" disclosures took place in closed groups during oral conversations, making it less likely for those disclosures to spread and be made available to others who might want to harm the client. In writing online, such disclosures can easily be spread and become exceedingly dangerous both to the client and to the integrity of the legal system.

An outrageous example of oversharing involves an assistant public defender in Illinois who posted sensitive client information on her blog, referring to clients by their first names and even revealing information relating to a client's drug use.[129] A less outrageous, but still problematic, example involved posting that the "the client just lied to me about a crucial fact - I hate it when they do that."[130] Such a post could "reveal confidences because the post has a date

---

http://www.abajournal.com/news/article/top_court_nixes_lawyers_request_for_reprimand_dismisses_case_due_to_lack/.

[129] Robert J. Ambrogi, *Lawyer Faces Discipline Over Blog Posts*, LAW.COM LEGAL BLOG WATCH (Sept. 11, 2009, 3:10 PM), http://legalblogwatch.typepad.com/legal_blog_watch/2009/09/lawyer-faces-discipline-over-blog-posts.html.

[130] Smith, *supra* note 54, at 7.

and a time, and a reader might well be able to identify which client [she was] meeting with."[131]

A thoughtful District of Columbia Ethics Opinion states that "[w]hile lawyers may ethically write about their cases on social media, lawyers must take care not to disclose confidential or secret client information in social media posts . . .," and that it is always necessary to obtain consent from the client before posting any details of their case online.[132]

Even if an attorney is reasonably certain that disclosures of case or client details will not be prohibited by the rules of his or her jurisdiction, it is always best to err on the side of caution in obtaining consent from the client.[133] Added complications arise where a lawyer posts on social media about a client, and then posts personal opinions on seemingly unrelated political or social topics that ultimately are adverse to the potential interests of the client.[134]

2. Reviews, Rankings, and Feedback

Another hotspot for disclosure mistakes arises with the trend of using the internet for feedback. A significant feature of the internet is a lawyer's ability to invite comments and ratings and clients' ability to gripe online. Lawyers have revealed confidential client information while responding to negative feedback on rating sites. One lawyer responded to a negative rating with this: "I dislike it very much when my clients lose, but I cannot invent positive facts for clients when they are not there. I feel badly for him, but his own actions in beating up a female co-worker are what caused the consequences he is now so upset about."[135] A lawyer may in self-defense spill out a justification that reveals too much about the case. When it happens in writing

[131] *Id.*
[132] *Id.*
[133] *Id.*
[134] *See Id.*
[135] *In re* Tsamis, No. 2013PR00095 (Ill. Att'y Registration and Disciplinary Comm'n Jan. 15, 2014), http://www.iardc.org/HB_RB_Disp_Html.asp?id=11221 (joint stipulation and recommendation for a reprimand by the hearing board); *see also* Debra Cassens Weiss, *Lawyer accused of revealing TMI in response to bad Avvo review is reprimanded; overdraft also cited*, A.B.A. J. (Jan. 21, 2014, 5:45 AM), http://www.abajournal.com/news/article/lawyer_who_revealed_tmi_in_response_to_bad_avvo_review_is_reprimanded/?utm_source=maestro&utm_medium=email&utm_campaign=weekly_email.

on a publicly accessible and easily duplicated and preserved medium, the harm is vastly enlarged.

In a culture where a company's online presence is just as, if not more, important than its physical presence, a bad review online can have a substantial impact. One lawyer in Utah decided that the best way to deal with a negative online review that stated he was the "[w]orst ever," among other things, was to sue the person who posted the review for "defamation, intentional infliction of emotional distress, and intentional interference with prospective economic relations."[136] The district court dismissed all of the claims and was upheld by the appellate court holding that the online review was merely an opinion and thus did not rise to the level of a tort.[137] The publicity from the suit brought far more attention to the negative review and did nothing to make this lawyer more appealing to future clients. As one blogger who covered the opinion said, "Spoiler alert: suing the client is not the correct answer."[138]

In responding to reviews of any nature, lawyers must be careful not to reveal client confidences. The District of Columbia for example permits lawyers to reveal client confidences only when responding to "'specific' allegations by the client concerning the lawyer's representation of the client."[139] D.C. rules also "specifically exclude[] general criticisms of an attorney from the kinds of allegations to which an attorney may respond using information otherwise protected. . . ."[140] The New York State Bar takes an even stricter stance and holds that, "[a] lawyer may not disclose confidential client information solely to respond to a former client's

[136] Spencer v. Glover, 397 P.3d 780, 783 (Utah Ct. App. 2017).
[137] *Id.*
[138] Eric Goldman, *How Should a Lawyer Respond to a Yelp Review Calling Him "Worst. Ever."?*, TECHNOLOGY & MARKETING LAW BLOG (Apr. 24, 2017), http://blog.ericgoldman.org/archives/2017/04/how-should-a-lawyer-respond-to-a-yelp-review-calling-him-worst-ever-spencer-v-glover.htm.
[139] D.C. Bar Ass'n, Ethics Op. 370, s*upra* note 32.
[140] *Id.*

criticism of the lawyer posted on a [lawyer-rating website]."[141]

3. Internet Provider Disclosures

Other risks arise with social media websites. Lawyers' three most commonly used social media networking sites are Facebook, Twitter, and especially LinkedIn. The ABA 2015 Techreport found that ninety-nine percent of large firms, ninety-seven percent of mid-size firms, ninety-four percent of small firms, and ninety-three percent of solo firms have a LinkedIn profile.[142] LinkedIn offer users the option to import contact information from an existing email account; doing this may "publicize details about clients, witnesses, consultants, and vendors."[143] Caution is warranted in such instances and confidentiality issues may arise because often times use of social media websites involves access to address books, and "allows the social media site to suggest potential connections with people the lawyer may know who are already members of the social network, to send requests or other invitations to have these contacts connect with the lawyer on that social network, or to invite non-members of the social network to join it and connect with the lawyer."[144] The reason why this can be a huge technoblunder is because,

> [I]n many instances, the people contained in a lawyer's address book or contact list are a blend of personal and professional contacts. Contact lists frequently include clients, opposing counsel, judges and others whom it may be impermissible, inappropriate or potentially embarrassing to have as a connection on a social networking site. The connection services provided by many social networks can be a good marketing and networking tool, but for attorneys, these connection services could potentially identify clients or divulge other information

[141] *Id.* (quoting N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Ethics Opinion 1032, Oct. 2014, http://www.nysba.org/CustomTemplates/Content.aspx?id=52969).
[142] Allison Shields, *Blogging and Social Media,* ABA TECHREPORT 2016, https://www.americanbar.org/publications/techreport/2016/social_media_blogging.html. ("In total, 78% of respondents report that their firms maintain a presence on LinkedIn. This represents a drop from previous years, when this number topped 90%. This could be due to a greater understanding on the part of respondents that a firm presence on LinkedIn (a law firm business page), may be different than firms requiring or encouraging their lawyers to complete their individual LinkedIn profiles, or it could mean that firms are not seeing the value of firm business pages on LinkedIn and prefer to focus more on individual lawyers[sic] profiles and networking to gain visibility for both the lawyers and the firm.")
[143] Lackey & Minta, *supra* note 127, at 155.
[144] DC Bar Ass'n, Ethics Op. 370: Social Media I: Marketing and Personal Use, Nov. 2016, http://www.dcbar.org/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm.

> that a lawyer might not want an adversary or a member of the judiciary to see or information that the lawyer is obligated to protect from disclosure. Accordingly, great caution should be exercised whenever a social networking site requests permission to access e-mail contacts or to send e-mail to the people in the lawyer's address book or contact list and care should be taken to avoid inadvertently agreeing to allow a third-party service access to a lawyer's address book or contacts.[145]

4. Unsecured Access

A major, but often unappreciated risk, arises from the prevalence of unsecured internet connections also raises confidentiality concerns. Lawyers and clients may send and receive digital communications on unsecured internet access services at a restaurant, park, airport, and other public locations. Some still have home wireless routers that do not require passwords. Someone on the street can access an inadequately protected internet access point, even from outside a building or home, and monitor communications.[146] If a party other than the lawyer, such as a spouse, child, or untrained staff member, uses a computer, phone, or email account, communications and stored information are not secure.

5. Terminated Devices

Another common problem involves lawyers, clients, and firm employees who exchange or sell devices, or return company owned equipment. A departing employee may return a device with digital information still on it, even if the employee tried to erase it. If the employee did not remove passwords or did not log out of accounts, privileged attorney-client messages could appear on the device now in the possession of another owner or former employer. One employee sued a former employer when he found out that his old company-issued iPhone, which he had returned to his former employer, was still linked to his Apple account.[147] The text messages he

---

[145] *Id.*
[146] Cheryl B. Preston, *WiFi in Utah: Legal and Social Issues*, UTAH BAR JOURNAL, Sept. & Oct. 2007, at 29.
[147] Venkat Balasubramani, *Employer Isn't Liable When Former Employee Linked His Apple Accounts To Its Devices–Sunbelt v. Victor*, TECH. & MARKETING L. BLOG (Sept. 18, 2014),

received on his new phone were automatically sent to the phone that was now in his former employer's possession.[148] This case did not involve a lawyer, but a lawyer or litigant could easily make the same mistake. In addition, devices may have been programmed to remember passwords or otherwise contain cookies that store and apply all kinds of information automatically, giving the new owner access to a host of personal data containing confidential information.

The Florida Bar, the leader in addressing technology, issued an ethics opinion on the proper ways to handle hard drives from discarded computer equipment to protect confidential client information.[149] The Florida Bar addressed the obligations of lawyers regarding information stored on hard drives in hopes of preventing the leak of confidential information. In an ethics opinion, the bar stated that "[h]ard drives from high speed scanners and other like computer equipment" may retain records of scanned documents that can be accessed after the equipment is discarded.[150] "[L]awyers…must take reasonable steps to ensure that client confidentiality is maintained and that the Device is sanitized before disposition."[151] Other bar associations need to incorporate similar warnings.

6. Ransomware

An increasingly common risk involves third parties who hack in and freezing lawyer's computer systems and demand a ransom be paid to unlock the system.[152] Although the payment

---

http://blog.ericgoldman.org/archives/2014/09/employer-isnt-liable-when-former-employee-linked-his-apple-accounts-to-its-devices-sunbelt-v-victor.htm.

[148] *Id*.

[149] Fla. Bar, Opinion 10-2, Sept. 24, 2010, http://www.floridabar.org/TFB/TFBETOpin.nsf/b2b76d49e9fd64a5852570050067a7af/b3861cd80f9b3c0b852577f8006ea7cf!OpenDocument (discussed in Jake Schickel, *A Report from the Florida Bar Board of Governors Meeting*, FIN. NEWS & DAILY REC. (June 7, 2010), http://www.jaxdailyrecord.com/showstory.php?Story_id=531175).

[150] *Id*.

[151] *Id*.

[152] Vanessa S. Browne-Barbour, *"Why Can't We Be 'Friends'?": Ethical Concerns in the Use of Social Media*, 57 S. TEX. L. REV. 551, 568 (2016) (giving examples of firms that have been subject to such attacks).

of the ransom does not itself raise ethical concerns, firms that are unable to pay the ransom risk the "or else" threat, which is the hackers will release the information into the public or permanently delete it. A public release results in a breach of confidentiality and permanent inability to access firm files dramatically affects a lawyer's ability to competently represent a client. Loss of records entrusted to a lawyer raises a plethora of common law and statutory claims from affected clients. The incidence of ransomeware attacks is rising. John Simek, the vice president at Sensei Enterprises Inc. said that "When it comes to ransomware . . . attacks are growing and that many firms end up having to pay the ransom because they didn't have systems in place to recover the stolen data. 'Our own clients are beginning to wake up to the fact that these types of attacks can happen anytime.'"[153]

In Rhode Island, the law firm Moses Afonso Ryan allegedly lost $700,000 in billings from a ransomware virus that infected the firm's computer network.[154] The virus was unwittingly introduced to the firm's network because a lawyer clicked on an infected email attachment which downloaded the virus and encrypted the law firm's network for three months until the ransom of $25,000 was paid to release the network.[155] The law firm had an insurance policy through Sentinel, which paid the maximum $20,000 as provided under the policy for virus coverage, but the policy would only cover "lost business income . . . when there is physical loss or damage to property at the business premises . . .."[156] Moses Afonso Ryan filed a claim against Sentinel for

[153] Victor Li, *How Prepared Are Law Firms for Cyber Breaches? And How Often Are Firms Being Attacked?*, A.B.A. J. (Jun. 29, 2017, 8:41 AM CDT), http://www.abajournal.com/news/article/how_prepared_are_law_firms_for_cyber_breaches_and_how_often_are_they_being_/?utm_source=maestro&utm_medium=email&utm_campaign=weekly_email.
[154] Debra Cassens Weiss, *Victimized by Ransomware, Law Firm Sues Insurer for $700K in Lost Billings*, A.B.A. J. (May 2, 2017 11:09 AM CDT), http://www.abajournal.com/news/article/victimized_by_ransomware_law_firm_sues_insurer_for_700k_in_lost_billings/.
[155] *Id.*
[156] *Id.*

the $700,000 in lost billings because of the virus.[157] Cases like these demonstrate how lawyers need to guard themselves against the risks of not only their unethical behavior, where purposeful or not, but also against the behavior of others who could use technology to extort money from a law firm, or compromise confidential client data.

5. Employer Access

A serious and not uncommon example involves the attorney who communicates with a client who is at work. Recently in California, a lawyer permitted a client who was involved in litigation with her employer to discuss the case, facts, and strategy from her workplace using her employer's equipment.[158] A company policy had warned that an email account "was to be used only for company business, that e-mails were not private, and that the company would randomly and periodically monitor its technology resources to ensure compliance with the policy."[159] The employee had been given the company's handbook and signed that she had read its terms.[160] Like the rest of us, she did not think twice about it again and fell into the common illusion that emails are private. Of course, the court determined that the emails were not private and therefore they were not protected by attorney-client privilege.[161] The employer could use against her any content it found.

The emerging view is that employees, like this client, have no reasonable expectation of privacy when using employer equipment or systems.[162] And even if there were a reasonable expectation of privacy, many companies require the employee to enter into an agreement regarding the terms of using the employer's equipment or Internet access. If an employee's email

[157] *Id.*
[158] *See* Holmes v. Petrovich Dev. Co., 119 Cal. Rptr. 3d 878 (Cal. Ct. App. 2011).
[159] *Id.* at 896.
[160] *Id.* at 883.
[161] *Id.* at 895.
[162] *See, e.g., id.*

address or IP address includes words or numbers relating to the employer, a reasonable employee should realize that the employer may have rights to access and use electronic communications.

6. Employee Access

A member of a lawyer's staff who has terminated employment at a firm or other business may retain passwords that allow continued access to company email and electronically stored information. If a dispute arises, or just curiosity, the former employee may seek to access digital information.[163] In a recent criminal complaint, Michael Potere, a former associate at Dentons, a Los Angeles law firm, was charged with extortion. Potere allegedly threatened to reveal sensitive firm documents that he had obtained by using the email password of a partner at Denton.[164] The email password was given to Potere when he worked on a case together with the partner in 2015.[165] Potere, upset about not being able to continue working at Dentons until the fall where he would start a political science degree program, "demand[ed] that the law firm pay him $210,000 and give him a piece of artwork to ensure the documents remained secret . . ."[166] This is a prime example of why lawyers must frequently change passwords, especially when employees are terminated.

In addition, lawyers should be warned about the frequent cases involving current employees allowing others to use their online identities or passwords that link and allow access to lawyer information. One attorney in West Virginia repeatedly accessed the emails of his wife and seven of his wife's co-workers at her law firm because he thought she was engaging in an

[163] *See, e.g.*, United States v. Morris, 928 F. 2d 504 (2d Cir. 1991).
[164] Debra Cassens Weiss, *Former Dentons associate accused in extortion plot involving threat to leak documents to legal blog*, A.B.A. J. ONLINE (June 28, 2017 9:47 AM CDT), http://www.abajournal.com/news/article/ex_dentons_associate_is_accused_in_extortion_plot_involving_threat_to_leak
[165] *Id.*
[166] *Id.*

extramarital affair.[167] There is no evidence in this case that the outside attorney was looking for client information, but if the fear had been that the wife was having an affair with a client, sensitive information on the client's legal matters may have been exposed. Spouses of employees may have legal access to passwords or share computers with cookies permitting access to private sites. Lawyers and firms need to be much more vigilant in policing employee access to client information.

Some kinds of employees and agents have access to computer systems or equipment for repair or maintenance purposes. Something available on the computer may tempt such a person to copy or use the information or disclose it to others. Anyone in the office may access a lawyer's computer and any open internet sites while the lawyer is out to lunch, in a conference, in the bathroom, etc. Of course, before the digital era, co-workers and maintenance staff could always have looked at papers on the desk or opened files and drawers. However, papers on a desk do not include a record of the user's search history or networks of stored information. Digital information can be searched by keyword easily and quickly. It can be printed, forwarded to another account, or saved on a flash drive. Moreover, someone with access to a lawyer's email account or blog may post information in the name of the lawyer or send out requests for information that may result in breaches to confidentiality.

7. Information Storage

Storing information in a cloud creates a risk of disclosing confidential client information.[168] In addition to large, sophisticated firms, the 2016 ABA Legal Technology Report found that forty-six percent of two-to-nine attorney firms and forty-two percent of solo practice

[167] Lawyer Disciplinary Bd. v. Markins, 663 S.E.2d 614, 615-17, 622 (W. Va. 2008).
[168] Martha Neil, *Potential Privilege Pitfalls Posed by Cloud Storage*, A.B.A. J. ONLINE (Sep 9, 2013 8:55 AM CDT), http://www.abajournal.com/news/article/online_doc_repositories.

attorneys use the cloud.[169] Outsider hacking of firm computer systems to obtain information on clients, potential stock offerings, and political dirt is a serious risk brought on with the use of technology.

A startling report released on June 27, 2017 by LogicForce, a cybersecurity firm, detailed just how "woefully unprepared" law firms are against cyber threats.[170] The report used data compiled from surveys and found that "77 percent of responding firms did not have cyber insurance, 95 percent of responding firms were noncompliant with their own cyber policies, 100 percent were noncompliant with a client's policies, and 53 percent of responding firms do not have a data breach incident response plan."[171] The report notes that, because of most law firm's dreadful state of unpreparedness, "It is truly not a question of if, but when, an incident will occur."[172] The risks go beyond a failure to keep client information private, and include the loss of the attorney/client privilege, loss of work product claims in discovery, and loss of trade secret protection. In addition, information exposed may be a violation of various securities laws and confidentiality agreements with third parties. Exposing client information opens up an attorney to a variety of common law and statutory claims. This Part discusses various information storage related technoblunders and their consequences.

Of critical concern is cloud storage. Much has been written elsewhere on the benefits and risks of attorneys using the cloud and this is not the place for a thorough exploration of all the implications. However, the risks are sufficiently substantial that mention of methods to protect

---

[169] Dennis Kennedy, *Cloud Computing*, ABA TECHREPORT 2016, https://www.americanbar.org/content/dam/aba/publications/techreport/2016/cloud/cloud-computing.authcheckdam.pdf (last visited Aug. 8, 2017).
[170] Victor Li, *How Prepared Are Law Firms for Cyber Breaches? And How Often Are Firms Being Attacked?*, A.B.A. J. (Jun. 29, 2017, 8:41 AM CDT), http://www.abajournal.com/news/article/how_prepared_are_law_firms_for_cyber_breaches_and_how_often_are_they_being_/?utm_source=maestro&utm_medium=email&utm_campaign=weekly_email.
[171] *Id.*
[172] *Id.*

stored information in professionalism creeds warrants discussion. In addition, internal firm computer systems and individual computers can be hacked.

In a 2016 case, a court held that an insurance company waived any privilege claim when it published confidential information onto an unprotected file-sharing site.[173] Even with ordinary precautions, electronic storage of large amounts of data is risky and history has amply shown that such data can be hacked.[174] In relation to trade secrets, Professor Sharon Sandeen has gone so far as to say, "The mere fact that you're storing on the cloud, in my opinion, is a strong argument that you've waived your trade secrecy."[175]

The ABA now "recognizes a . . . world where law enforcement discusses hacking and data loss in terms of "when," and not "if,"[176] and offers an insurance policy to cover cyber-incidents, including network extortion.[177] A press release noted:

> In recent years, the legal profession has become a popular target for hackers. Despite vigilance and increased awareness by law firms and individual lawyers, cyber-related risks have escalated based on the sensitivity and nefarious uses of that data. Last year, for example, the Manhattan U.S. attorney's office unsealed indictments against three Chinese men who are accused of using stolen law firm employee credentials to access troves of internal emails at two law firms. The men, according to prosecutors, used details they obtained from partners' emails about pending deals to make more than $4 million in illegal stock trades.[178]

One study estimated that eighty percent of the 100 largest law firms have had a malicious

[173] Harleysville Ins. Co. v. Holding Funeral Home, Inc., No. 1:15CV00057, 2016 WL 4703755 (W.D. Va. Sept. 8, 2016).
[174] *Id.*; Victor Li, *Tools for Lawyers Worried that NSA is Eavesdropping on Their Confidential Conversations*, A.B.A. J. (Mar. 30, 2014 12:44 PM), http://www.abajournal.com/news/article/tools_for_lawyers_worried_that_nsa_is_eavesdropping_on_their_confidential_c/.
[175] *Id.*
[176] American Bar Association Standing Committee on Ethics and Professional Responsibility, Formal Opinion 477R*, Securing Communication of Protected Client Information (revised May 22, 2017), https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.authcheckdam.pdf (referencing THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS (2013)).
[177] ABA begins offering cyber liability insurance to lawyers, law firms of all sizes, A.B.A., Mon Feb 27 13:30:03 CST , 2017, https://www.americanbar.org/news/abanews/aba-news-archives/2017/02/aba_begins_offering.html.
[178] *Id.*

computer breach during a one-year period.[179] Some of these may include ordinary phishing scams, but an occasional employee falls for the ploy and reveals confidential information.[180] Some have been major breaches with serious confidentiality implications and may result in class action lawsuits against the firms.[181]

Another risk of storing large amounts of data in the cloud is access to the information by the service provider. Recently, Google introduced a free service called Optical Character Recognition (OCR) that extracts information from documents and images stored in your drive to make your files more searchable.[182] Google uses information to trigger advertising and sells user data to others. Some commentators suggest that "lawyers should avoid using free email or cloud storage services like Gmail and Dropbox. The free versions allow Google and Dropbox to scan everything sent to the service, which compromises client confidentiality."[183] While Google may use client information for advertising, a potentially greater risk is that Google Drives may be hacked.

8. Reasonable Efforts to Protect

Following the 2012 amendments, Model Rule 1.6(c) provides: "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized

---

[179] Matthew Goldstein, *Law Firms are Pressed on Security for Data*, N.Y. TIMES (Mar. 26, 2014), http://dealbook.nytimes.com/2014/03/26/law-firms-scrutinized-as-hacking-increases/?_php=true&_type=blogs&_php=true&_type=blogs&_php=true&_type=blogs&_php=true&_type=blogs&emc=edit_tnt_20140326&nlid=1166199&tntemail0=y&_r=3. See also Lisa Morgan, *Panama Papers Fallout: What If Your Lawyer Gets Hacked?*, INFO. WEEK, May 31,2016, http://www.informationweek.com/strategic-cio/security-and-risk-strategy/panama-papers-fallout-what-if-your-lawyer-gets-hacked/a/d-id/1325545 (identifying various firms suffering data breaches).

[180] Waqas Amir, *Google Docs Users Targeted with "Confidential Document" Phishing Scam*, HACKREAD (July 9, 2015, 4:51 AM), https://www.hackread.com/google-docs-phishing-scam/.

[181] Gabe Freeman, *Threats of litigation after data breaches at major law firms*, Mar/ 30, 2016, Bloomburg Law-Big Law-Business, https://bol.bna.com/threats-of-litigation-after-data-breaches-at-major-law-firms/ (reporting on data breaches at Weil Gotshal & Manges and Gravath, Swaine & Moore and other firms).

[182] *About Optical Character Recognition in Google Drive*, GOOGLE DRIVE HELP, https://support.google.com/drive/answer/176692?hl=en (last visited Sept. 8, 2015).

[183] Tsutomu Johnson, *Sorry I Lost Your Files: Cybersecurity Threats to Confidentiality*, 28 UTAH B. J., July-Aug. 2015, at 41-43.

access to, information relating to the representation of a client."[184] At least nineteen state and local ethics opinions have addressed the question of cloud-based information storage, and all have decided that it is ethically permissible to use cloud storage services, but only if attorneys use "reasonable care."[185] The problems with this advice that lawyers may not be alert to the risks and will not seek out advice from ethics opinions and, more importantly, there are no concrete standards for "reasonable care." Each opinion notes different specific obligations of attorneys to shield against confidentiality concerns.[186] Vague recommendations obligations include taking reasonable security precautions by weighing the sensitivity of the data, the impact of disclosure on the client, the urgency of the situation, and the client's instructions; and ensuring cloud providers have enforceable obligations to preserve confidentiality and security. One thing is clear: the failure to take any precautions certainly is a violation of the duty of confidentiality. And failure to respond appropriately once a system is hacked is another risk, as Yahoo!'s top lawyer can attest.[187] In addition, lawyers need to be reminded of the obvious professional duty to report data breaches to clients, who are the real victims of these kinds of attacks.

When the ABA amended Model Rule 1.6, rather than clarlify a position reconciling or directing the suggestions in various bar associations statement on cloud computing and rather than giving lawyers a clear standard for what is "reasonable," it chose to give vague and limited guidance in the Comment to Rule 1.6.[188] "A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized

[184] MODEL RULES OF PROF'L CONDUCT r. 1.6(c) (AM. BAR ASS'N 2013).
[185] *Cloud Ethics Opinions Around the U.S.*, A.B.A., http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html#AZ (last visited May 30, 2014).
[186] *Id.; see also* Geraghty & Micchmerhuizen, *supra* note 127, at 559-60.
[187] Vindu Goel*, Yahoo's Top Lawyer Resigns and C.E.O. Marissa Mayer Loses Bonus in Wake of Hack,* N.Y.T, Mar. 1, 2017, Https://Www.Nytimes.Com/2017/03/01/Technology/Yahoo-Hack-Lawyer-Resigns-Ceo-Bonus.Html?Smid=Pl-Share&_R=0.
[188] MODEL RULES OF PROF'L CONDUCT r. 1.6 cmts. 16–17 (AM. BAR ASS'N).

disclosure . . . . When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients." Lawyers' views of "reasonable" depends on their awareness of the risks, which is still doubtful, and their awareness of the easily available security options.

Unfortunately, the Comment begins by ignoring the facts of modern practice and lulling lawyers into believing that "This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy."[189] The Comment admits that "special circumstances . . . warrant special precautions," and offers a list of extremely vague factors. First is the "sensitivity of the information." What information about a lawyer's representation of a client is not per se "sensitive," other than what can be reported in the newspaper, such as scheduling and published court orders, and friendly chitchat? The Comment also reminds lawyers that some information is "protected by law or by a confidentiality agreement."[190] The Model Rule 1.6 Comment does not educate or guide lawyers by identifying various laws that protect information. Moreover, all attorney-client information is protected by a "confidentially agreement" imposed as a matter of common law, if not ethics rules.

Other factors include "the likelihood of disclosure if additional safeguards are not employed."[191] Like speeding, not everyone gets caught, but the risks of disclosure are broad and cannot be denied. Another factor is "the cost of employing additional safeguards [and] the difficulty of implementing the safeguards."[192] While technoneophytes likely think that

[189] ABA Formal Opinion 477 (2017).
[190] *Id.*
[191] *Id.*
[192] *Id.*

investigating and implementing security measures is daunting, the 2017 ABA Opinion 477 acknowledges

> a variety of options to safeguard communications including, for example, using secure internet access methods to communicate, access and store client information . . . , using unique complex passwords, changed periodically, implementing firewalls and anti-Malware/AntiSpyware/Antivirus software on all devices upon which client confidential information is transmitted or stored, and applying all necessary security patches and updates to operational and communications software. Each of these measures is *routinely accessible and reasonably affordable or free*."[193]

Why not *require* the use of measures that, at any given time, are "routinely accessible and reasonably affordable or free" or at least provide a list of the kinds of simple, low cost measures that are available? At a minimum the ABA Model Rules should address the use of unsecured networks and public wifi and the risk of unsuspectingly downloading viruses.

The last factor found in the Rule 1.6 Comment for determining the level of security necessary factor is "the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use)."[194] The Comment thus offers an easy excuse, without acknowledging that almost none of the routinely available security measures make anything "excessively difficult to use." Moreover, ample examples in this Article and elsewhere show that some lawyers believe that avoiding unsecured networks, restricting posts on social media, occasionally changing passwords, and avoiding cell phones for sensitive communications is just too difficult. Some lawyers may think that giving up the convenience of discussing client matters with a colleague in

[193] American Bar Association Standing Committee on Ethics and Professional Responsibility, Formal Opinion 477R*, Securing Communication of Protected Client Information (revised May 22, 2017), https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.authcheckdam.pdf (emphasis added).
[194] *Id.*

a crowded elevator or at a bar makes practice excessively difficult, but that has never been an excuse.

In an attempt to add some specificity to the woefully inadequate Comment to Rule 1.6, the ABA recently issued ABA Formal Opinion 477. It adds various tips about obvious risks and is a starting point for training lawyers, even though it offers no more concrete standards than in the Comment to Rule 1.6. Opinion 477 mentions the well-known fact that "client [may use] computers or other devices subject to the access or control of a third party," and it reminds lawyers of their duties to supervise staff and nonlawyers to whom work is delegated. Finally, in addition to other "may"s and "should"s, Opinion 477 suggests a "better practice" of marking communications "privileged and confidential." Such disclaimers are usually at the bottom and not noticeable until the message has been read in full. In addition, those with a financial or strategic stake in the legal matter are unlikely to immediately delete it, even if they had not already read the contents.

Opinion 477 lists in footnote various lawsuits involving the breach of confidentiality by electronic communications,[195] but nothing in the Opinion sets a standard stronger than "reasonable" but undefined steps to avoid these or other risks.[196]

Another step that should be required as a reasonable effort to protect against technoblunders is a requirement for lawyers to become aware of the policies of online platforms and services and then avoid those whose policies allow the provider wide powers to access information and relieve the provider from giving information to others or other mishandling of

[195] E.g., Scott v. Beth Israel Med. Center, Inc., Civ. A. No. 3:04-CV-139-RJC-DCK, 847 N.Y.S.2d 436 (Sup. Ct. 2007); Mason v. ILS Tech., LLC, 2008 WL 731557, 2008 BL 298576 (W.D.N.C. 2008); Holmes v. Petrovich Dev Co., LLC, 191 Cal. App. 4th 1047 (2011) (employee communications with lawyer over company owned computer not privileged); Bingham v. BayCare Health Sys., 2016 WL 3917513, 2016 BL 233476 (M.D. Fla. July 20, 2016) (collecting cases on privilege waiver for privileged emails sent or received through an employer's email server).
[196] *Id.*

information. The District of Columbia bar recently addressed an issue few if any lawyers have grasped.[197] It stated, "It is critically important that lawyers review the policies of the social media sites that they frequent, particularly policies related to data collection. Privacy settings on social media are not the equivalent of a guarantee of confidentiality." Lawyers, as with all other internet users, will resist taking the time to find the providers terms on their webpages, read the lengthy statement, and understand how the policies relate to risks.[198] Even if the policies were initially read, lawyers do not keep up on the regularly changing terms even if they have notice of the changes. Bar associations might provide the service of reviewing the policies of popular social media cites and advise lawyers of the specific risks. Certainly professionalism standards in each jurisdiction should specifically alert lawyers to the risks created by common online provider contracts and advise against using platforms with certain terms or a history of disclosures.

Although using two-step passwords and encryption is a better practice, a minimum step that should be required is strengthening and protecting passwords. Risks abound. For instance, the Heartbleed bug, which allowed third parties to potentially view encrypted data, affected

---

[197] DC Op. 371.

[198] NANCY S. KIM, WRAP CONTRACTS: FOUNDATIONS AND RAMIFICATIONS 1, 213 (2013) (citations omitted):

> One study estimated that it would cost the average American Internet user 201 hours or the equivalent of $3,534 a year to read the privacy policies of each website that he or she visits. . . . [Y]ou would not have time to engage in productive work, recreational activities, or relationships. Modern life, in other words, would break down if we treated wrap contracts just like other contracts.[198]

See also Cheryl B. Preston, *"Please Note: You Have Waived Everything": Can Notice Redeem Online Contracts?*, 64 AM. U. L. REV. 535, 552-62 (2015) (citations omitted):

> In addition to time drain, a second reason not to read wrap contracts is that they are difficult, dense texts. Most readers cannot be expected to comprehend them even if they read every word. Wrap contracts are increasingly elaborate, monotonous, and written in ways that suggest the drafter intended to obfuscate the scariest parts by embedding them in excess verbiage and repetition. Remember, wrap contract drafters do not have to worry about printer or paper costs, mailing or storage costs, or the cautionary impact of presenting a long paper contract to a consumer in its obvious fullness. Key sections in wrap contracts are frequently presented in all capital letters, but that does not help.

many sites that could contain sensitive information, such as Yahoo!, Google, Box, and Dropbox, as well as other sites that cater specifically to lawyers.[199] One commentator opined that, at a minimum, ethics required lawyers to change their passwords.[200]

Requiring particular methods of security runs the risk of becoming outdated, but the Model Rules or state professionalism standards can require the use of at least one of a variety of methods subject to advances in the field. Without federal legislation, the bar can adopt standards for ethical behavior that draw on the specifics in The Sarbanes Oxley Act (SOX),[201] Federal Information Security Management Act (FISMA),[202] Family Educational Rights and Privacy Act (FERPA),[203] Gramm Leach Bliley Act (GLBA),[204] or Payment Card Industry Data Security Standard (PCI-DSS) administered by the Payment Card Industry Security Standards Council.[205]

Bar association standards can, at a minimum, advise lawyers who are not technologically sophisticated and employing existing security measures to get professional advice on securing communications and cloud storage from an information systems expert. If a disclosure or breach occurs, a lawyer's failure to have reasonable security measures in place should be an ethics violation subject to bar disciplinary action. Bar associations could also require continuing legal education hours in the subject of communications and information security.

Language setting forth the most minimum of standards that can be added to bar association standards is as follows:

---

[199] Robert Ambrogi, *Which Legal Sites Did Heartbleed Affect?*, L. SITES (April 14, 2014), http://www.lawsitesblog.com/2014/04/legal-sites-heartbleed-affect.html.
[200] Aaron Street, *Heartbleed: What Lawyers and Law Firms Need to Know*, LAWYERIST (April 11, 2014), http://lawyerist.com/72733/heartbleed-lawyers-law-firms-need-to-know/ (suggesting encrypting and backing up hard drives).
[201] 15 U.S.C.A. §§ 78a et seq.
[202] 44 U.S.C.A §§ 3145 et seq.
[203] 20 U.S.C. §§ 1232g et seq.
[204] Public Law 106–102, 113 Stat. 1338, 1999, adding to and amending various sections of Titles 12 and 15 U.S.C.A, https://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf (last visited Aug. 2, 2017.
[205] Payment Card Industry Security Standards Council, https://www.pcisecuritystandards.org/pci_security/ (last visited Aug. 2, 2017).

> Lawyers should be alert to the increased risk of interception of, and unauthorized access to, digital communications and information storage, including the risks of unauthorized access, unintended disclosure of details that can be aggregated, and oversharing of personal information or activities that might allude in any way to clients and cases. Lawyers should carefully screen any information posted to social media sites. Lawyers should use frequently changed and robust passwords, two-factor authentication, or encryption. Unless technologically sophisticated or advised by a security expert, lawyers should not store client information on the cloud. Lawyers should not use unsecured internet access points or routers to discuss client business. Lawyers should consider cyber liability insurance.
>
> Lawyers are responsible for failures to protection information from improper use by employees, agents, and repair service technicians who have access to electronic devices on which may be stored client information. Lawyers should discuss with, and obtain consent from, clients regarding the use of electronic communications in various circumstances. Lawyers should request that clients store and discuss case details only on reasonably secure devices and provide clear advice about the risks of social media.

C. Rule 1.7(b)and(c):Conflicts of Interest

Rule 1.7(b)(4) prohibits representing a client with respect to a matter if "the lawyer's professional judgment on behalf of the client will be or reasonably may be adversely affected by . . . the lawyer's own financial, business, property or personal interests," unless the conflict is resolved in accordance with Rule 1.7(c). Posts on social media may take a position that is contrary to the interests of a current or potential client. The District of Columbia bar warns about such inadvertent creations of conflicts and notes that even "the acquisition of uninvited information through social media cites could create actual or perceived conflicts of interest for the lawyer or the lawyer's firm." Lawyers and firms often run legal updates where they may opine on the merits of a new legislation or a recent case. Others run opinionated blogs as a way of attracting clients or garnering social and peer acceptance for positions taken by existing major clients.

Professionalism standards adopted by bar associations should include:

> Lawyer or firm postings on social media, as well as third party comments

(invited or uninvited) may create subject matter conflicts even if a future client is not adverse to a prior client.

D. Rule 3: Obstruction and Extrajudicial Statements

1. Rule 3.4(a):Obstruction and Spoilation of Evidence.

Model Rule 3.4(a) creates the duty not to "[o]bstruct another party's access to evidence or alter, destroy, or conceal evidence, or counsel or assist another person to do so. . . ."[206] Copies of electronic communications should be preserved in the client's file. The District of Columbia Ethics Opinion 370 adds a further twist. "Social media sites may not permanently retain messages or other communications; therefore care should be taken to preserve these communications outside of the social media site, in order to ensure that the communications are maintained as part of the client file."**[207]** In addition to keeping their own records, lawyers must warn clients of the consequences resulting from spoliation of evidence,[208] including sanctions including adverse inference at trial, assessment of costs and fees, disciplinary action, default judgment, as well as tort and criminal liability.[209] Professor Browne-Barbour cites several cases, ethics opinions, and commentators that discuss spoliation.[210]

In addition, District of Columbia Ethics Opinion 371 warns that the law, which varies

---

[206] MODEL RULES OF PROF'L CONDUCT r. 3.4(a) (AM. BAR ASS'N 2013).

[207] The D.C. Bar Association also recommends that lawyer-client communications be made through a secure office email rather than social media because, "Social media sites may not permanently retain messages or other communications; therefore care should be taken to preserve these communications outside of the social media site, in order to ensure that the communications are maintained as part of the client file." D.C. Bar Ass'n, Ethics Op. 370, *supra* note 32.

[208] Browne-Barbour, *supra* note 146, at 575 (citations omitted).

[209] *Id.*

[210] *Id.* (citing *e.g.*, Gatto v. United Airlines, Inc., No. 10-CV-1090-ES-SCM, 2013 WL 1285285, at *1 (D.N.J. Mar. 25, 2013); Patel v. Havana Bar, Rest. & Catering, No. 10-1383, 2011 WL 6029983, at *1 (E.D. Pa. Dec. 5, 2011); Lester v. Allied Concrete Co. (*Lester II*), Nos. CL08-150, CL09-223, 2011 WL 9688369, at *1 (Va. Cir. Ct. Oct. 21, 2011), *aff'd in part, rev'd in part*, 736 S.E.2d 699 (Va. 2013); Prof 1 Ethics Comm. of the Fla. Bar, Proposed Advisory Op. 14-1 (2015); Pa. Bar Ass'n Comm. on Legal Ethics & Prof 1 Responsibility, Formal Op. 2014-300, at 7 (2014); Phila. Bar Ass'n Prof 1 Guidance Comm., Op. 2014-5 (2014); N.Y. Cnty. Lawyers Ass'n Comm. on Profl Ethics, Ethics Op. 745, at 3 (2013); N.C. State Bar Ethics Comm., 2014 Formal Ethics Op. 5 (2014); John G. Browning, *A Clean Slate or a Trip to the Disciplinary Board? Ethical Considerations in Advising Clients to 'Clean Up' Their Social Media Profiles*, 48 CREIGHTON L. REV. 763, 763-64 (2015); John G. Browning & Al Harrison, *"What Is That Doing on Facebook?!": A Guide to Advising Clients to 'Clean Up' Their Social Media Profiles*, HOUS. LAW., Jan./Feb. 2016, at 26, 27; John Levin, *Social Media-Advising Your Client*, CBA REC., Jan. 2015, at 40, 40; Agnieszka McPeak, *Social Media Snooping and Its Ethical Bounds*, 46 ARIZ. ST. L.J. 845, 888-94 (2014)).

among jurisdictions, may prevent advising a client to "modify their social media presence once litigation or regulatory proceedings are anticipated."[211] Lawyers must consult obstruction statutes, spoliation law, procedural rules for criminal and regulatory investigations, and rules for civil cases before taking down or advising clients to take down social media posts.[212] The time to advise clients about the risk that information in social media will come back to haunt them is before it is posted.

2. Rule 3.6: Extrajudicial Statements by Non-Prosecutors

Model Rule 3.6 provides: "A lawyer . . . shall not make an extrajudicial statement that the lawyer knows or reasonably should know will be disseminated by means of public communication and will have a substantial likelihood of materially prejudicing an adjudicative proceeding in the matter."[213] The Rule expressly details the limited kinds of information that can and cannot be revealed. Being in front of a television camera or talking to a reporter would put most lawyers on alert to carefully monitor information disclosed. However, in this generation, every lawyer can actually *be* the press. At any time, including while sitting at counsel table, a lawyer may, with a few thumb strokes, broadcast a message to untold millions. Hopefully, it is unlikely a lawyer would actually intend to broadcast the information about the legal proceeding to inappropriate parties, but the belief that a tweet or text will be kept private is unfounded.

Already situations involving lawyer communications during judicial proceedings are coming to light. The harm is compounded if the lawyer is an employee of the government working for the court. For instance, a court research attorney tweeted during an attorney discipline proceeding her take on the merits of the case and the moral turpitude of the respondent

[211] D.C. Bar Ass'n, Ethics Op. 371, *supra* note 32.
[212] *Id.* (citations omitted).
[213] MODEL RULES OF PROF'L CONDUCT r. 3.6 (AM. BAR ASS'N 2013).

Phill Kline:[214] "Why is Phil Klein [sic] smiling? There is nothing to smile about douchebag," "ARE YOU FREAKING KIDDING ME. WHERE ARE THE VICTIMS? ALL THE PEOPLE WITH THE RECORDS WHO [sic] WERE STOLEN," "I predict that he will be disbarred for a period not less than 7 years," and finally, "It's over . . . sorry. I did like how the district court judges didn't speak the entire time. Thanks for kicking out the SC Phil [sic]! Good call!"[215] The bar association reprimanded the tweeting attorney, finding that her prediction was a misrepresentation of fact and law, implied that she had undue influence over the judges, disrespected a litigant, disrespected the judges, and prejudiced the administration of justice.[216] This consequence of a mere reprimand seems inadequate to address such a breach. This behavior throws the legal system in disrepute because of the implication that a party involved in the proceeding was subject to a general bias and not able to obtain a fair outcome.

A new standard can remind lawyers that their online communications during a proceeding are inappropriate.

> Communication via social media platforms by lawyers and court personnel constitutes "public communication." Lawyers must avoid extrajudicial statements via social media platforms that the lawyer knows or reasonably should know will have a substantial likelihood of materially prejudicing an adjudicative proceeding in the matter.

3. Rule 3.8: Extrajudicial Statements by Prosecutors

Rule 3.8 provides "The prosecutor in a criminal case shall . . . refrain from making extrajudicial comments that have a substantial likelihood of heightening public condemnation of the accused."[217] There are already reported cases involving prosecutor tweets made during a trial.

[214] *In re* Sarah Peterson Herr, Final Hearing Report (Jan. 13, 2014), http://www.kscourts.org/pdf/Herr-Admonition-Final-Report.pdf.
[215] *Id.*
[216] *Id.*
[217] MODEL RULES OF PROF'L CONDUCT r. 3.8 (AM. BAR ASS'N 2013). In addition to the Rule, thirty states have adopted a standard encouraging honesty. Preston & Lawrence *supra* note 11, at tbl.3.

One case was based on these tweets: "I have respect for attys who defend child rapists. Our system of justice demands it, but I couldn't do it. No way, no how," and "Jury now has David Polk case. I hope the victim gets justice, even though 20 years late."[218] The appellate court that considered the prosecutor's tweets did not decide whether they were improper since the real test is whether the trial was fair.[219] However, the judge mentioned that the timing and content of the messages increased the likelihood that a jury would be tainted.[220] Aside from tainting the jury, providing information to the public that predicts a result or suggests facts not elicited in the evidence is covered by the intent of Rule 3.8. The question arises of whether prosecutors can risk posting anything on the internet relevant to any cases.[221]

A new standard can remind prosecutors that online social media communications are public, and thus there is great risk of abuse when commenting about an ongoing case. A standard might look like this:

> Prosecutors should know that online social media posts are public extrajudicial comments. As such, prosecutors should ensure that their social media posts (i) do not have a substantial likelihood of heightening public condemnation of the accused and (ii) do not have a substantial likelihood of tainting a jury.

E. Rules 3.4, 4.1, 4.4, and 5.3: Abuse of the Research Process

Model Rule 3.4 requires parties to act in fairness during the discovery process.[222] This Rule was originally addressed to abusively large and detailed discovery requests intended to require excessive and unnecessary effort and expense of the other party. This problem is vastly magnified with the ease of generating electronic requests and the vastly increased amounts of digitally stored data.

---

[218] Missouri v. Polk, 415 S.W.3d 692, 695 (Mo. App. E.D. 2013).
[219] *Id.* at 696.
[220] *Id.*
[221] Emily Anne Vance, Note, *Should Prosecutors Blog, Post, or Tweet?: The Need for Hew Restraints in Light of Social Media*, 84 FORDHAM L. REV. 367 (2015).
[222] MODEL RULES OF PROF'L CONDUCT r. 3.4 (AM. BAR ASS'N 2013).

Something new and insufficiently addressed, however, are abuses involved with electronic fact research regarding opposing parties, opposing attorneys, judges, jurors, or witnesses. In a recent study, eighty-one percent of attorneys who responded used evidence from social media in their cases.[223] "Facebook was found to be the most popular source of evidence, with 66% of attorneys responding indicating that they had used evidence found on the site."[224] Some argue that a lawyer who does not take advantage of the vast new resources for discovery is guilty of malpractice.[225] One court recently held that it was not only acceptable, but good practice, for attorneys to bring their laptops to the courtroom and conduct searches while potential jurors are being questioned.[226] Because of the potential for online factual research, lawyers should warn their clients to post only truthful statements, encourage clients to avoid posting information that could be detrimental, and provide guidelines for taking down information.[227]

This vast body of potential evidence comes with the risk of various abuses. For example, some courts do not allow questions about political affiliations, but this information is often available on social media web pages.[228] Some courts and commentators express concern that, when jurors know that lawyers use various means, especially online, to find information about

[223] Zoe Rosenthal, *"Sharing" with the Court: The Discoverability of Private Social Media Accounts in Civil Litigation*, 25 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 227, 229 (2014) (footnote omitted).
[224] *Id.*
[225] *See, e.g.,* Shannon Awsumb, *Social Networking Sites: The Next E-Discovery Frontier*, 66 BENCH & BAR OF MINN. (Nov. 2009), http://www2.mnbar.org/benchandbar/2009/nov09/networking.html ("[A]ttorneys should explore social networking sites as part of their formal and informal discovery efforts and case preparation. Just as it would be unthinkable nowadays to conduct discovery without considering what email evidence may be available, attorneys should give the same attention to social networking information to ensure that all smoking guns have been uncovered and addressed.").
[226] *See* Carino v. Muenzen, No. L-0028-07, 2010 WL 3448071 (N.J. Super. Ct. App. Div. Aug. 30, 2010) ("That he had the foresight to bring his laptop computer to court, and defense counsel did not, simply cannot serve as a basis for judicial intervention in the name of 'fairness' or maintaining 'a level playing field.'").
[227] N.Y. Cty. Law. Ass'n, *Advising a Client Regarding Posts on Social Media Sites*, Op. 745, NYCLA.org (July 2, 2013) https://www.nycla.org/siteFiles/Publications/Publications1630_0.pdf.
[228] Robert B. Gibson, *Researching Jurors on the Internet—Ethical Implications*, N.Y. ST. B.J. Nov.–Dec. 2012, at 10, 12 ("Now, through the Internet, trial attorneys can obtain information about prospective jurors that would otherwise not be disclosed during voir dire , such as the juror's political beliefs and economic philosophies.").

jurors, some people would be discouraged from jury duty.[229] Other issues involving research are even more serious.

Finding and using information that is publicly available online is legitimate.[230] "Lawyers, just like everyone else, are freely permitted to search social media for information concerning a litigant and to view the information that is generally available to the public."[231] However attempts to gain access to private social media accounts, blogs, and chat rooms are generally improper. This includes the actions of third parties at the direction of the lawyer.

Most lawyers are not experts in internet law nor do they carefully think through the implications of the Model Rules when applied to novel techniques. Lawyers should be warned about how easy and tempting overreaching is online and reminded that their behavior may be exposed even if lawyers believe they act anonymously. The implications of improper conduct affect the reputation of the lawyer personally and the legal system as a whole if their conduct is exposed.

The use of any kind of intentional deception to obtain advantage in the legal system should be strictly prohibited. A person who sees a communication not knowing it came from a lawyer or a person involved in a legal process cannot weigh the credibility of the information or recognize harmful strategic behavior. When doing research, lawyers must avoid making any communication with a judge or a person represented by counsel as covered by Model Rules

---

[229] *See, e.g.*, Report on N.Y. City Bar Ass'n Comm. on Prof'l & Judicial Ethics, Op. 2012-02 (May 2012) http://www.nycbar.org/member-and-career-services/committees/reports-listing/reports/detail/formal-opinion-2012-2-jury-research-and-social-media ("[J]urors who understand that many of their social networking posts and pages are public may be discouraged from jury service by the knowledge that attorneys and judges can and will conduct active research on them or learn of their online—albeit public— social lives.").

[230] *See, e.g.*, Oregon State Bar Legal Ethics Comm., Op. 2005-164, 453 (2005) (finding that accessing an opposing party's public website does not violate the ethics rules and is conceptually no different from reading a magazine article or purchasing a book written by that adverse party.)

[231] John M. Flannery, *The Discoverability and Admissibility of Social Media in NY Civil Litigation*, *in* NEW DEVELOPMENTS IN EVIDENTIARY LAW IN NEW YORK 3, 3 (2013) (footnote omitted).

3.5(b) and 4.2. Ex parte communications of this sort, including "friending" in that context, are discussed in Subpart III F.

A. Friending

Lawyers are tempted to send friend requests under their names but without disclosing the lawyers' interest in a case as some people accept friend requests indiscriminately. Several state and local bar associations have addressed friending specifically. The San Diego Bar Association concluded that "friending" potential witnesses without disclosing the purpose of the request is unethical, even when using a true name.[232] The Pennsylvania, New Hampshire, and Philadelphia Bar Associations have found that viewing the public portions of a Facebook profile is ethical, but requesting access to a private profile is inappropriate.[233]

However the New York City Bar Association reached a different conclusion.[234] If a real name appears on the friend request, it is not making a false statement.[235] "Consistent with the policy [in favor of informal discovery], we conclude that an attorney or her agent may use her real name and profile to send a 'friend request' to obtain information from an unrepresented person's social networking website without also disclosing the reasons for making the request,"[236] as long as it does not include any kind of misrepresentation. The opinion draws the following analogy:

---

[232] San Diego County Bar Legal Ethics Comm., Op. 2011-2 (May 24, 2011).
[233] Pennsylvania Bar Ass'n Legal Ethics Comm., Op. 2014-300 (Sept. 2014); New Hampshire Bar Ass'n Ethics Comm., Advisory Opinion 2012-13/05 (2012) ("There is a split of authority on this issue, but the Committee concludes that such conduct violates the New Hampshire Rules of Professional Conduct."); Philadelphia Bar Ass'n, Op. 2009-02 (2009) (finding that directing a third party to friend a witness using only truthful information, "omits a highly material fact, namely, that the third party who asks to be allowed access to the witness's pages is doing so only because he or she is intent on obtaining information and sharing it with a lawyer for use in a lawsuit to impeach the testimony of the witness"); *see also* Steven C. Bennett, *Ethical Limitations on Informal Discovery of Social Media Information*, 36 AM. J. TRIAL ADVOC. 473, 484 (2013) (discussing a Philadelphia bar opinion).
[234] N.Y.C. Bar Ass'n, Formal Op. 2010-2 (2010), http://www.nycbar.org/member-and-career-services/committees/reports-listing/reports/detail/formal-opinion-2010-02-obtaining-evidence-from-social-networking-websites.
[235] *Id.*
[236] *Id.*

> If a stranger made an unsolicited face-to-face request to a potential witness for permission to enter the witness's home, view the witness's photographs and video files, learn the witness's relationship status, religious views and date of birth, and review the witness's personal diary, the witness almost certainly would slam the door shut and perhaps even call the police.
>
> In contrast, in the "virtual" world, the same stranger is more likely to be able to gain admission to an individual's personal webpage and have unfettered access to most, if not all, of the foregoing information.[237]

Unlike the opinion's holding, this reasoning suggests that, because we are not as careful in granting friend requests as we are with opening our door even though the results could be similar, friending to garner evidence or private information are never proper.

Furthermore, regarding technology abuse in research, lawyers must be warned that directing someone else to do it does not remove liability. Responsibility lies with the lawyer even if an agent, employee, or other third party takes the action. Rule 5.3 (b) - (c)(1) states:

> (b) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and
>
> (c) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:
>
> > (1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved.[238]

For example, while representing defendants in a personal injury lawsuit, two attorneys directed a paralegal to gather information about the plaintiff using the internet.[239] The plaintiff's Facebook page was initially public, and the paralegal accessed it multiple times.[240] When the plaintiff's profile became private, the attorneys directed the paralegal to continue to monitor the plaintiff's social media activity by sending him a "friend request."[241] While the paralegal did not

[237] *Id.*
[238] Model Rules of Prof'l Conduct r. 5.3 (b)-(c)(1) (Am. Bar Ass'n (2002).
[239] Robertelli v. New Jersey Office of Atty. Ethics, 134 A.3d 963, 965 (N.J. 2016).
[240] *Id.*
[241] *Id.*

use a false identity, she also did not disclose that she worked for the law firm representing the defendants in the pending lawsuit.[242] When the attorneys sought to introduce the paralegal as a trial witness and introduce documents from the plaintiff's Facebook page, the plaintiff filed an ethical grievance complaint with the state Ethics Committee.[243] Although the New Jersey Supreme Court did not directly decide whether the attorneys committed an ethical violation by requesting their paralegal to "friend" an opposing party, it did hold that the Office of Attorney Ethics could prosecute the alleged misconduct.[244]

While clients are not under the same obligations as lawyers, lawyers are obligated to advise clients to avoid overreaching, illegal or fraudulent conduct, or trying to communicate with a party represented by counsel.[245] Lawyers, however, are fully responsible for using information improperly obtained by a client. Recently, the Missouri Supreme Court indefinitely suspended a lawyer for using information in a divorce case that was obtained by his client after guessing his wife's email password.[246]

B. False Names and Identities

Most opinions so far focus on deceptive friending. Several Model Rules touch on misrepresentations. Model Rule 4.1 provides: "In the course of representing a client a lawyer shall not knowingly . . . make a false statement of material fact or law to a third person."[247] Model Rule 4.4 provides: "[A] lawyer shall not use . . . methods of obtaining evidence that

---

[242] *Id.*
[243] *Id.*
[244] *Id.* at 975.
[245] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 11-461 (2011) (warning that lawyers must advise their clients, that when communicating with other parties, they should not overreach or interfere with the other party's client-lawyer relationship).
[246] *In re* Eisenstein, 485 S.W.3d 759, 761 (Mo. 2016) (en banc). One judge wrote a dissenting opinion, joined by one other judge, arguing that the attorney's violation of various Model Rules warranted a suspension with no leave to apply for reinstatement for twelve months. *Id.* at 164.
[247] MODEL RULES OF PROF'L CONDUCT r. 4.1 (AM. BAR ASS'N 2014).

violate the legal rights of such a person."[248] In addition, Model Rule 8.4 addresses fraud. Using subterfuge for purposes of gathering information is addressed in a variety of formal opinions.[249] Even the New York City Bar Association held that using falsehoods to obtain evidence is unethical.[250] "[F]or example, an attorney may not claim to be an alumnus of a school that she did not attend in order to view a juror's personal webpage that is accessible only to members of a certain alumni network."[251] In one example, a lawyer in a wrongful discharge action sought access under a false identity to the social media pages of a client's co-workers in hopes of finding others disparaging the employer.[252]

Although a variety of similar deceptions likely occurred in cases before the internet, especially those involving private investigators, the simple and relatively costless methods of obtaining information online make this temptation significantly more powerful. In the real world, people do not generally give personal information to strangers indiscriminately, but people online are much less careful and lawyers should not abuse their misjudgment.

C. Entrapping Disclosures

Of even greater concern are attempts by a lawyer (or a lawyer's agent or client) to direct the conversation on blogs, chatrooms, and other social media sites for the purpose of inducing comments or information that otherwise may not have been posted. In 2013, a prosecutor created a fake Facebook profile and pretended to be the ex-girlfriend of a defendant in a murder case to

[248] MODEL RULES OF PROF'L CONDUCT r. 4.4(a) (AM. BAR ASS'N 2013).
[249] *See, e.g.*, Oregon Bar, Formal Op. 2013-189 (2013) ("Lawyer may not engage in subterfuge designed to shield Lawyer's identity from the person when making the request.").
[250] N.Y. City Bar Ass'n Comm. on Prof'l & Judicial Ethics, Op. 2010-02 (Sept. 2010).
[251] *Id.*
[252] John G. Browning, *Digging for the Digital Dirt: Discovery and Use of Evidence From Social Media Sites*, SMU SCI. & TECH. L. REV. 465, 477–48 (2011).

get two witnesses to change their story about the defendant's alibi via the chat feature on Facebook.[253]

Another issue with available technology involves recording conversations without the consent of all the parties to the conversation. In most state and federal jurisdictions, it is not illegal to secretly record a conversation as long as at least one party to the conversation (the party recording) has consented.[254] Although lawyers were generally forbidden from making such recordings without disclosure to other parties, the American Bar Association reversed this position in a formal opinion.[255] It concluded that, although discouraged, secret recordings are not misconduct per se as long as it is not illegal to do so in a lawyer's respective jurisdiction. "A lawyer who electronically records a conversation without the knowledge of the other party or parties to the conversation does not necessarily violate the Model Rules."[256] The previous opinion was based upon "the principle that a lawyer 'should avoid even the appearance of impropriety.'"[257] The ABA withdrew its previous opinion because an "overwhelming majority of states permit recording by consent of only one party to the conversation" and there may be legitimate reasons for making a record to avoid fraud.[258] Although the ABA changed its position, it continues to advise against recording exchanges with clients without their knowledge, and

[253] Aaron Brockler, *Former Prosecutor, Fired For Posing As Accused Killer's Ex-Girlfriend On Facebook*, HUFFINGTON POST (June 7, 2013, 2:25 PM), http://www.huffingtonpost.com/2013/06/07/aaron-brockler-fired-facebook_n_3402625.html.

[254] *E.g.*, 18 U.S.C.S. § 2511 (LexisNexis 2017) ("It shall not be unlawful . . . for a person . . . to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception . . ."); Ariz. Rev. Stat. § 13-3005 (LexisNexis 2017); D.C. Code § 23-542 (LexisNexis 2017); N.Y. Penal Law § 250.00 (LexisNexis 2017).

[255] Electronic Recordings by Lawyers Without The Knowledge of All Participants, ABA Formal Op. 01-422 , June 24, 2001, https://www.americanbar.org/groups/professional_responsibility/publications/ethics_opinions/index_by_issue_dates.html (replacing ABA Formal Op. 337 which in part stated that "with a possible exception for conduct by law enforcement officials, a lawyer ethically may not record any conversation by electronic means without the prior knowledge of all parties to the conversation.").

[256] *Id.*

[257] *Id.*

[258] *Id.*

outright forbids any representation that a conversation is not being recorded when in actuality it is.[259] With the ABA, most state bar associations discourage secret recordings and remind lawyers that the totality of circumstances surrounding the recording may suggest the lawyers has engaged in dishonesty, fraud, deceit, or misrepresentation in violation of Model Rule 8.4(c).[260]

Sometimes lawyers, even judges, show undue enthusiasm for recording devices. For instance, in New Mexico, the Attorney General has charged dismissed Magistrate Court Judge Connie Johnston in connection with recording telephone conversations within secure, nonpublic areas of the courthouse without the participants' consent and involving multiple people.[261] In Kansas City a federal prosecutor lost her job at the U.S. Attorney's office because she had listened to recordings of private conversations between a Leavenworth inmate and his lawyer provided by a private prison company.[262] Lawyers must recognize that covert recordings bring many hazards.

D. Hacking

Some lawyers may have superior technological skills. Bar associations should take the lead in warning them that gaining unauthorized access to another's electronic communications and computers is not merely an ethical issue, but is also illegal. In addition to prohibiting intentional interception during an electronic transmission without a court order,[263] the Stored Communications Act makes it illegal to access electronic communications in an inbox, outbox or otherwise stored without authorization from the owner (or to intentionally exceed authorized

---

[259] *Id.*
[260] *See, e.g.*, Utah State Bar Ass'n, Ethics Advisory Op. No. 96-04, Dec. 18, 1997; Ohio State Bar Ass'n, Op. 2012-1.
[261] Joshua Kellogg, *AG Files Charges Against Aztec Judge*, Farmington N.M. Daily T., July 29, 2017, at 1A.
[262] Debra Cassens Weiss, *Federal prosecutor admits she listened to recordings of attorney-client conversations, filing says*, A.B.A. J. ONLINE (June 29, 2017 7:00 AM CDT), http://www.abajournal.com/news/article/federal_prosecutor_admits_she_listened_to_recordings_of_attorney_client_con/?utm_source=maestro&utm_medium=email&utm_campaign=weekly_email.
[263] 18 U.S.C.A. § 2511(1).

access) and thereby obtain, alter, or prevent authorized access to a wire or electronic communication.[264]

The Computer Fraud and Abuse Act[265] makes unauthorized access to another's computer for an improper purpose a crime. Subsection 1030(a)(2)(C) is surprisingly broad and, by its terms, makes it a crime to exceed authorized access of a computer connected to the internet *without* any culpable intent. Although some courts are unlikely to interpret minor violations as a crime,[266] lawyers should stay well within the law when doing research on the case facts, parties, judges, or jurors.

The following is possible language addressing this concern for use in professionalism standards:

> Lawyers can and should search social media in the formal and informal discovery processes. However, lawyers should not seek to gain access to a private social media account by use of misleading statements or false names nor should they direct others under their control to do so. Even "friending" the subjects of their inquiries without a clear disclosure of the lawyers' identity and purpose can be misleading. Lawyers who comment online should avoid using potentially deceptive methods, such as false identities, to mislead others as to the source of online statements.

F. Rule 3.4(b): Coaching Witnesses

Another issue made critical because of electronic communications is sending messages to other participants during a proceeding. It seems not to fit well in any of the Model Rules. The closest is Rule 3.4(b), which prohibits assisting a witness to testify falsely. Some professionalism creeds forbid lawyers from coaching witnesses or obstructing a deposition and such language,[267] including direct reference to tweets and electronic chats during testimony should be added to all

[264] 18 U.S.C.A. § 2701.
[265] 18 U.S.C.A. § 1020.
[266] United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc).
[267] *See* UTAH STANDARDS OF PROFESSIONALISM & CIVILITY r. 18 (2014). Six states have this standard. Preston & Lawrence *supra* note 11, at tbl.7.

creeds. When the Model Rules were written, improper coaching was hard to define and limited to discussion during preparation time or breaks, and rambling objections.[268] It would have been impossible for a lawyer to coach a witness in specific terms in real time.

Today, witnesses and lawyers can hold cell phones under a table and discreetly text a witness in a deposition or in trial, especially in video depositions. Technically the Model Rules only address assisting false testimony; but leading a witness to give responses that the witness did not come up with on his or her own is false and certainly misleading testimony.[269] For example, a lawyer in Michigan and his client in California exchanged five text messages while the client was being deposed via videoconference.[270] The only reason the exchange came to light is because the lawyer accidentally sent a text meant for his client to opposing counsel in New Jersey.[271]

Hopefully, the Model Rules will be amended to provide more specific coverage about inappropriate digital communication during testimony, but in the meantime, this temptation must be addressed in bar association standards. One option is to provide:

> During depositions and testimony lawyers should not obstruct the interrogator or object to questions unless reasonably intended to preserve an objection or protect a privilege for resolution by the court. "Speaking objections" designed to coach a witness are impermissible. This includes using technology to send any communication to, or receive any from, a witness, lawyer, or other participant. During depositions or conferences, lawyers shall engage only in conduct that would be appropriate in full sight of a judge.

G. Rules 3.5 and 4.2: Ex Parte Communications

[268] Tom Barber, *Restrictions on Lawyers Communicating with Witnesses During Testimony: Law, Lore, Opinions, and the Rule*, FLA. B.J., July/Aug. 2009, at 58, https://www.floridabar.org/DIVCOM/JN/JNJournal01.nsf/Author/F361C04FC87E0EF2852575D600654478.
[269] Richard C. Wydick, *The Ethics of Witness Coaching*, 17 CARDOZO L. REV. 1, 3–4 (1995); Barber, *supra* note203, at 58, 60.
[270] Wei Ngai v. Old Navy, 2009 U.S. Dist. LEXIS 67117 (D.N.J. 2009).
[271] *Id.* at 2.

Model Rules 3.5(a) and (b) prohibits ex parte communication with "a judge, juror, prospective juror or other official by means prohibited by law" and "with such a person during the proceeding unless authorized to do so by law or court order." Model Rule 4.2 prohibits communicating directly with anyone represented by counsel.[272] Given the ease and ubiquity of digital communications, the opportunities for unintended improper communications and the magnitude of harms they may cause are significantly increased in cyberspace. Indeed, some lawyers may intentionally use electronic means to send "hints" and "thoughts" to persons covered by these Rules. Because of the increased risks and subtleties of electronic messaging, intentional and unintentional communication by social media must be directly confronted, defined, and prohibited rather than relying on lawyers to register how such behavior might fit under Model Rules 3.5 and 4.2.

Recognizing the ease with which a lawyer can communicate with a juror online, the New York City Bar Association has urged lawyers use extreme caution when researching jurors in the course of a trial. [273] Its formal opinion warned, "[R]esearching jurors mid-trial is not without risk. For instance, while an inadvertent communication with a venire member may result in an embarrassing revelation to a court and a disqualified panelist, a communication with a juror during trial can cause a mistrial."[274] Several professionalism creeds include language addressing the prohibition on ex parte communications, but none implicate the heretofore impossible ways that a simple online click could constitute a communication.[275] An affirmative attempt to engage

[272] UTAH STANDARDS OF PROFESSIONALISM & CIVILITY r. 11 (2014). Fourteen states mention this in their standards, in addition to being a violation of the Rules of Professional Conduct. Preston & Lawrence *supra* note 11, at tbl.6.
[273] Ass'n Bar City of New York Comm. on Prof'l Ethics, Formal Op. 2012-02 (May 2012), http://www.nycbar.org/ethics/ethics-opinions-local/2012opinions/1479-formal-opinion-2012-02.
[274] *Id.*
[275] UTAH STANDARDS OF PROFESSIONALISM & CIVILITY r. 11 (2014). Fourteen states mention this in their standards, in addition to it being a violation of the Rules of Professional Conduct. Preston & Lawrence, *supra* note 11, at tbl.6.

in ex parte communications about a case through use of social media is clearly inappropriate, even if the facts and identities are veiled.

The ways in which messages can be communicated electronically are so varied, I discuss several of them specifically.

1. Friending

The subject of friending for purposes of research on parties, jurors, and witnesses is discussed in detail above in Subpart III D. In addition to the problems described in that Subpart, using the various techniques of social media associations also risks violating the rules governing ex parte communications.

Sending a connection/access invitation (such as a "friend request" on Facebook) is widely regarded as a communication, even though it is a simply a click of the mouse and no words are exchanged. The ABA's Formal Opinion 466 states that, for purposes of Model Rule 3.5, a lawyer may review a juror's or potential juror's public postings, but should not send a request for access to private sites, directly or indirectly. This applies to lawyers and to anyone acting on their behalf.[276] The ABA offers a parable for explanation:

> This would be the type of ex parte communication prohibited by Model Rule 3.5(b). This would be akin to driving down the juror's street, stopping the car, getting out, and asking the juror for permission to look inside the juror's house because the lawyer cannot see enough when just driving past.[277]

A New Hampshire Bar formal opinion reminds us that attempting to communicate with a witness in the same matter involving a lawyer's client is also an improper ex parte communication that implicates Model Rule 4.2.[278]

2. Follower Notifications

[276] ABA Comm. on Ethics & Prof'l Responsibility, *supra* note 32.
[277] ABA Comm. on Ethics & Prof'l Responsibility, *supra* note 32.
[278] New Hampshire Bar Ass'n, Op. 2012-13/05 (2012) ("If the witness is represented by a lawyer with regard to the same matter in which the lawyer represents the client, the lawyer may not communicate with the witness except as provided in Rule 4.2.").

Some sites, such as LinkedIn, send a notification to users when a third party views their profile.[279] This is relevant when a lawyer is researching a juror, represented party, or judge. Ethics opinions are split on whether this constitutes a communication.[280] In a formal opinion, the ABA states that since the automatic notification is generated by the website, it "is akin to a neighbor's recognizing a lawyer's car driving down the juror's street and telling the juror that the lawyer had been seen driving down the street."[281] The lawyer's actions may seem invasive, discourage serving on juries, and suggest a threat. The New York City Bar Association adopted a broad definition of the word "communicate," and concluded that automatic notifications are a communication because "at a minimum, the researcher imparted to the person being researched the knowledge that he or she is being investigated."[282] Of course, researching opposing parties, the assigned judge, and a lawyer's own clients is good practice.[283] But attorneys must be cautious about the implications of any notice generated by the attorney that is conveyed to a third party.[284]

---

[279] However, the individual attorney can adjust his or her settings on LinkedIn to tailor what the user sees about the lawyer. *See "Who's Viewed Your Profile" - Privacy Settings*, LINKEDIN, https://help.linkedin.com/app/answers/detail/a_id/47992/ft/eng (last visited Sept. 3, 2015). There are three options:

1. "Your name and headline (Recommended)." *What Others See When You've Viewed Their Profile*, LINKEDIN, http://www.linkedin.com (last visited Sept. 3, 2015).
2. "Anonymous profile characteristics such as industry and title." *Id.*
3. "You will be totally anonymous." *Id.*

If an attorney chooses one of the latter two options, however, the "Profile Stats" feature (which allows users to tell who has viewed their profile) will be disabled for the attorney's account. *Id.* Essentially, if attorneys do not want that notification to the third party to contain any information about them, then they have to be willing to disable the setting that allows them to see who has been viewing their profile. In the ABA Techreport 2016, "76% of respondents report that they individually use or maintain a presence in one or more social networks for professional purposes. This number has also remained relatively steady since 2013." Shields, *supra* note 74. Obviously, in a profession that is so dependent upon networking, disabling this feature on a personal account could be detrimental, and is therefore not a viable option.

[280] ABA Comm. on Ethics & Prof'l Responsibility, *supra* note 32.

[281] ABA Comm. on Ethics & Prof'l Responsibility, *supra* note 32.

[282] The Ass'n of the Bar of the City of New York Comm. on Prof'l Ethics, *supra* note 208.

[283] Some have even opined that it is "bordering on malpractice" not to use the Internet in jury selection. Carol J. Williams, *Jury duty? May Want to Edit Online Profile; Trial Consultants Increasingly Use the Internet to Learn About Prospective Jurors*, L.A. TIMES, Sept. 29, 2008, at A6, http://articles.latimes.com/2008/sep/29/nation/na-jury29/2.

[284] Robinson, *supra* note 166, 637–38 (warning that attorneys should "be careful to ensure that their online research does not result in a communication").

One way to determine whether an online action should count as a prohibited "communication" is if the notification can be construed an intentional effort to send a "message," no matter how subtle.[285] If this is the pertinent distinction, passively viewing a profile that automatically generates a notification is not a communication, but actively requesting a friend status is. Not all commentators make this distinction. But lawyers deserve better guidance on what is appropriate.

3. Public Posts Intended as Messages

Even if there is no communication targeted at a specific party, juror, judge, or witness, putting information out on the internet still may lead to a communication that raises ethical issues. A unique opportunity for public concern arises with lawyers' online ability to communicate overt and covert messages through online postings that are likely to reach parties interested in a case. In some circumstances tweeting falls into the prohibition against public communications by a prosecutor,[286] discussed above in Subpart III C as well as the prohibition on ex parte communications. In one example, a prosecutor tweeted updates before, during, and after a trial.[287] On appeal, the defense argued that the verdict should be overturned because the prosecutor's tweets prejudiced the jury.[288] The appellate court did not find prejudice, but voiced concerns that such actions could taint the jury:

> [E]xtraneous statements on Twitter or other forms of social media, particularly during the time frame of the trial, can taint the jury and result in reversal of the verdict. We are especially troubled by the timing of [the prosecutor]'s Twitter posts, because broadcasting such statements immediately before and during trial greatly magnifies the risk that a jury will be tainted by undue extrajudicial influences.[289]

[285] *Id.* (recommending that the rules may "need to be more flexible regarding sites . . . which automatically notify a user when someone looks at their profile, with no other action by the user viewing the information.").
[286] MODEL RULES OF PROF'L CONDUCT r. 3.8 (AM. BAR ASS'N 2013).
[287] State v. Polk, 415 S.W.3d 692, 695 (Mo. Ct. App. 2013).
[288] Id.
[289] *Polk*, 415 S.W.3d at 695-96. Even though the court saw potential for harm with this behavior, it did not overturn the verdict because there was no evidence that the jury had been biased. *Id.* at 696.

This example serves to show that a lawyer making indirect communications may fail to assess the likelihood that online communications will spread beyond their intended recipients.

Currently, much of a lawyer's correspondence is digital.[290] As discussed above in Part II, one risk of digital information is accidently forwarding an email, or "replying all," without realizing a judge, court official, witness, or party is on the recipient list. Recall the example of a seasoned attorney who accidently sent an email with negative comments about the court to the chief judge.[291] The judge treated the email as an improper ex parte communication.[292]

A more subtle violation would be posting a copy of correspondence, or a summary of it, on a blog or social media site. The digitized image or text can easily be viewed by, or shown to, judges or members of the judge's staff. As we discuss below, many lawyers and judges have connected on social media websites. Even if the judge is not likely to see the post, the lawyer may know that a friend or family of the judge may see the post and pass it on. Traditionally, this kind of indirect communication would have required much more effort. A lawyer would have to start a rumor or give a copy to someone she believes will pass it on. Online, transmitting such information to anyone and everyone is fast, simple, and can include exact language. Many lawyers seriously underestimate how online posts and emails can be spread to potentially wide audiences. On the other hand, some lawyers may be fully aware of these patterns and intend to send a message to the judge through indirect means.

For example, after the Supreme Court's decision in *Kennedy v. Louisiana*,[293] a legal blogger found an error in the Court's opinion.[294] An attorney saw the blog post and mentioned it

[290] LEGAL TECHNOLOGY SURVEY REPORT, *supra* note 1, at 62.
[291] Patrice, *supra* note 105.
[292] *Id.*
[293] Kennedy v. Louisiana, 554 U.S. 407 (2008).
[294] Rachel C. Lee, Note, *Ex Parte Blogging: The Legal Ethics of Supreme Court Advocacy in the Internet Era*, 61

to his wife, a *New York Times* reporter, who then wrote a front-page story about the Court's mistake.[295] This eventually led to the court issuing an amended opinion, even though the outcome of the case was the same.[296] Although in this instance the blogger was an attorney that was not representing either party in the case, it is not far-fetched to imagine a scenario where counsel for one of the parties posts something online about an ongoing case in hopes that the content gets back to the court. In high-profile Supreme Court litigation, this possibility is not too remote. SCOTUSblog, a popular Supreme Court blog, was accessed "over a hundred" times in one day from an IP address registered to the Court.[297] This suggests that members of the Court or their staff are receiving the information included on the blog. Clearly, "the line between talking *about* the Court and talking *to* the Court" becomes blurred at times.[298]

A standard can warn of the risks of ex parte communications:

> Lawyers should be aware that communicating using digital mediums increases the risk of ex parte communications by inadvertently or intentionally sending a message or a copy of a correspondence to a judge or judicial staff through an indirect route online.
> When conducting informal fact research online, lawyers should not do anything that might be interpreted as sending a message or ex parte communication to judges, jurors, identified witnesses, or represented parties. This includes a request to connect, "friending," and other nonverbal actions that send a message to the recipient. It is always permissible to view publicly available information online. Since any online post has a potential of reaching unintended recipients, once a jury has been selected lawyers should avoid posts, tweets, and social media messages with content relevant to the case.

H. Rule 5.5: Unauthorized Practice of Law

STAN. L. REV. 1535, 1537-38 (2009).
[295] *Id.* at 1538.
[296] *Id.* at 1539-40.
[297] *Id.* at 1542 ("Of course, these visits could be from court personnel other than the Justices and their clerks, and some of the visits could be merely to peruse the court calendar or read coverage of a recently released decision. But a steady visitor to the site will be exposed to lists of cert petitions to watch, discussions of the filed briefs in various cases, and recaps of oral arguments, along with links to news stories or other blogs with similar material—all touching on the merits of pending litigation.").
[298] *Id.* at 1541 (emphasis added).

Model Rule 5.5(a) includes: "A lawyer shall not practice law in a jurisdiction in violation of the regulation of the legal profession in that jurisdiction."[299] Comment 4 adds" "Presence may be systematic and continuous even if the lawyer is not present [in the jurisdiction]." A looming risk that accompanies the wonder of a webpage presence is the unauthorized practice of law. Related risks are misleading information about a lawyer's services, discussed in Subpart III F, and violation of advertising regulations, discussed in Subpart III G. This Subpart focuses on when a web presence constitutes practice in jurisdictions where the lawyer is not licensed. While the treatment of unauthorized practice is clear under the Model Rules, what virtual activities constitute the practice of law is enormously confusing. Lawyers need clear guidelines.

Any offer of legal advice online raises the risk of unauthorized practice.[300] Webpages and online form services may constitute the practice of law in certain circumstances. Although this problem may seem obvious to some lawyers, other lawyers who set up webpages with legal information as a public service or as an inducement to attract clients seem to forget that a webpage reaches potentially every jurisdiction in the world. This issue becomes significantly more troubling when either the lawyer intends to attract non-residents or, when that is not the intent, the webpage is interactive and the host should have realized that an out-of-jurisdiction visitor to the website would rely on the posted information. For example, an appellate court in Indiana stated that attorneys consent "to the establishment of an attorney-client relationship if there is proof of detrimental reliance, when the person seeking legal services reasonably relies on the attorney to provide them and the attorney, aware of such reliance, does nothing to negate it . . . ,,[301]

[299] MODEL RULES OF PROF'L CONDUCT r. 5.5(a) (AM. BAR ASS'N 2014).
[300] Geraghty & Michmerhuizen, *supra* note 127, at 571-72.
[301] Hacker v. Holland, 570 N.E.2d 951, 956 (Ind. Ct. App. 1991) (quoting *Kurtenbach v. Tekippe*, 260 N.W.2d 53, 56 (Iowa 1977)).

This hypothetical situation demonstrates the problem of giving advice online. When an Idaho resident felt his rights had been violated by the police, he turned to the internet for an answer regarding how long he would have to bring a lawsuit in his jurisdiction.[302] The answer was provided by a lawyer in Wyoming who told the Idahoan that he had one year to bring suit, which would have been accurate if the man lived in Wyoming instead of Idaho.[303] However, when the man tried to bring his suit nine months later, he unpleasantly found out that the online advice he received was inaccurate for his jurisdiction, and that in Idaho he only had 180 days to bring his claim.[304]

The lawyer in this hypothetical could have, and should have been more careful to identify the jurisdiction of the person to whom he or she was giving legal advice to, rather than to just assume that the person was in a Wyoming jurisdiction. Furthermore, the lawyer in the hypothetical may not have even intended a lawyer-client relationship regardless of the residence of the questioner. If a lawyer's statement regarding the statute of limitations had not been given in response to a question, it may still have created problems. Lawyers who give specific statements of law may be inducing reliance and thus creating an attorney-client relationship and, if it is online and the applicable jurisdiction is not specified, the advice would be false and be malpractice.

This caution describes well the risks of creating a lawyer and client relationship online:

> Lawyers should be cautious not to create an unintended attorney-client cyber relationship. Having a conversation via social media and offering legal advice in that manner is one way that this could happen. To the extent that social media involves two-way communication, the possibility exists that a lawyer might unintentionally form an attorney-client relationship through social media. Lawyers accordingly should avoid creating an impression that they are providing

[302] This hypothetical is from Kristine M. Moriarty, Comment, *Law Practice and the Internet: The Ethnical Implications that Arise from Multijurisdictional Online Legal Service*, 39 IDAHO L. REV. 431, 432-33 (2003).
[303] *Id.*
[304] *Id.*

> legal services with their social media when they do not intend to do so. Although lawyers may give legal information to members of the public, such information can be transformed into legal advice if the lawyer applies analysis of the law to the particular facts of an individual's situation. Having a conversation on social media might accidentally trap an attorney into being deemed to have provided legal advice to someone he did not think was his client. If an individual reasonably believes that a lawyer has undertaken representation, the lawyer can be liable for negligence in providing the legal service and be subject to disciplinary action.[305]

Model Rule 8.5(b)(2) offers a safe harbor to mitigate the scope of the risk: "A lawyer shall not be subject to discipline if the lawyer's conduct conforms to the rules of a jurisdiction in which the lawyer reasonably believes the predominant effect of the lawyer's conduct will occur."[306] The D.C. ethics opinion however is quick to note that this model rule has not been adopted in every state, thus the caution for lawyers to do their due diligence in familiarizing themselves with surrounding jurisdiction's rules.[307]

The ABA 20/20 Commission proposed the following amendment to the Model Rules 5.5 Comments:

> For example, a lawyer may direct electronic or other forms of communications to potential clients in this jurisdiction and consequently establish a substantial practice representing clients in this jurisdiction, but without a physical presence here. At some point, such a virtual presence in this jurisdiction may become systematic and continuous within the meaning of Rule 5.5(b)(1).[308]

Unfortunately, this language was not adopted, apparently because of the fear that it would "chill cross-border practice."[309] A similar refusal to act involved the Connecticut Bar 2009 Task Force

---

[305] Thomas Roe Frazer II, *Social Media: From Discovery to Marketing-A Primer for Lawyers*, 36 AM. J. TRIAL ADVOC. 539, 564-65 (2013) (citations omitted).
[306] ABA Model Rule 8.5(b)(2).
[307] *Id*.
[308] Initial Resolution Model Rule 5.5(d)(3)/Continuous and Systematic Presence, ABA Comm'n on Ethics 20-20, at 2-3 (Sept. 7, 2011), available at http:// www.americanbar.org/content/dam/aba/administrative/ethics_2020/20110907_final_ ethics_2020_rule_5_5_d3_continuous_presence_initial_resolution_and_report_for_ comment.authcheckdam.pdf.
[309] See N.Y. St. Bar Ass'n Comm. Standards Atty Conduct, Comments on Ethics 20/20 Draft Reports Dated September 7, 2011, N.Y. State Bar Ass'n Comm. on Standards of Attorney Conduct (Nov. 21, 2011), available at http:// www.americanbar.org/content/dam/aba/administrative/ethics_2020/ethics_20_20_

on Unauthorized Practice Law on the Internet.[310] Although the task force concluded that several internet sites involved the unauthorized practice of law, it deferred to the administrative consumer protection agency rather than pursue action because the task force wanted to "avoid any unintended interference with ongoing efforts to nurture unbundled legal services."[311]

The problem is that webpages with legal advice are sprouting like mushrooms and attorneys are left without warning of the risks of creating a virtual presence in all the jurisdictions serviced by a webpage. Because practitioners with virtual offices can offer complete legal services, the foundational question arises of why licenses are required for having a physical office in a state.[312] The ABA and bar associations cannot continue to ignore these issues.

Cases finding the unauthorized practice of law in an online context have already arisen. A California court acknowledged these issues when it held that "an out-of-state lawyer's use of [electronic communications] could constitute unauthorized practice of law."[313] Other courts have addressed virtual practice problems. A recent example is *In re Brandes* where a New York appeals court held that a disbarred lawyer who provided service over the internet involving legal advice and contracting to draft briefs was engaged in unauthorized practice of law.[314] The Supreme Court of Nebraska held that an operator of a website selling presentations on eviction law engaged in the unauthorized practice of law.[315] Although the website operator in this case was not a lawyer, a licensed offering similar services online could be deemed practicing in each jurisdiction where customers reside. The principal office of Low Cost Paralegal Services was in

---

comments/newyorkstatebarassociationcommitteeonsta_initialdraftproposalonrule1._6_5_5_d_3_1_7_andadmissionbymotion.authcheckdam.pdf.

[310] CBA Task Force on Unauthorized Practice Law on the Internet, Interim Report, July 22, 2009.

[311] *Id.* at n.15.

[312] Stephen Gillers, *How to Make Rules for Lawyers: The Professional Responsibility of The Legal Profession*, 40 PEPP. L. REV. 365. 413-14 (2013).

[313] Stephen C. Bennett, *Ethics of Lawyer Social Networking*, 73 ALA. L. REV. 113, 128 (2009).

[314] In re Brandes, 28 N.Y.3d 1041 (Ct. App. N.Y. 2016).

[315] State ex rel. Commission on Unauthorized Practice of Law v. Hansen, 834 N.W.2d 793 (Neb. 2013).

Texas,[316] but its services were offered online to takers from other states. The Rhode Island Unauthorized Practice of Law Committee found that the operators of the webpage were engaging in the unauthorized practice of law, a finding affirmed by the Rhode Island Supreme Court.[317] The court further recommended that its order be turned over to the attorney generals of Rhode Island and Texas, the North Carolina State Bar, and the federal agency with jurisdiction over internet-based fraud.[318] A bankruptcy court in Montana ruled that the operator of an internet website through which debtors were advised of available exemptions and the site solicited information from debtors, was engaged in the unauthorized practice of law.[319] In an unpublished opinion the North Carolina Superior Court found that statements on a website included with a lien filing service constituted providing legal advice.[320]

The most notable case involved the legal forms offered by LegalZoon.com, Inc.[321] After various law suits and appeals, a district court in Missouri held that the legal document preparation service on the its website constituted the unauthorized practice of law.[322] Some of the cases were settled and others were dismissed based on the settlement.[323] In any event, lawyers with an online presence must carefully study what statements made and services offered constitute providing legal services and thus give rise to unauthorized practice claims in states where a lawyer is unlicensed.

---

[316] In re Low Cost Paralegal Services, 19 A.3d 1229 (R.I. 2011).
[317] *Id.*
[318] *Id.*
[319] In re Bagley, 433 B.R. 325 (Br. Mont. 2010).
[320] North Carolina State Bar v. Lienguard, Inc., 2014 WL 1365418 (N.C. Super. Ct. 2014) (not reported).
[321] For more discussion of the various law suits involve LegalZoom and similar webpages, see Raymond H. Brescia, et al., *Embracing Disruption: How Technological Change in The Delivery of Legal Services Can Improve Access to Justice*, 78 ALB. L. REV. 553, 583-85 (2014-15).
[322] Janson v. LegalZoom.com, Inc., 802 F.2d 1053 (W.D. Mo. 2011
[323] Webster, v. LegalZoom, 2014 WL 4908639 (Ct. App. 2d Ca. 2014) (not reported). The North Carolina court granted full faith and credit to the Webster settlement to terminate the LegalZoom case in its jurisdiction. Bergenstock v. LegalZoom.com, Inc., 2015 WL 2345453 (Sup. Ct. N.C. 2015) (not reported).

The language of some state ethics rules can be interpreted to address virtual offices, but the results are inconsistent.[324] For instance, Colorado allows lawyers from other jurisdictions to practice Colorado law, as long as they do not have a "domicile" or "a place for the regular practice of law" in the state.[325] In Virginia, out-of-state lawyers can have an office in Virginia without a Virginia license as long as they do not practice Virginia law. [326]This language seems to suggest that a virtual office may create the "systematic and continuous presence" for the practice of Virginia law even without any physical presence.[327] These regulatory positions were not written to specifically cover online legal services and are inadequate to give lawyers sufficient notice on the extent to which an online presence is considered the practice of law within a state.

Other unauthorized practice of law issues arise when software designed to assist in legal matters is offered for sale online. Of course, nonlawyers who make these forms available or who use them may be engaged in unauthorized practice.[328] The users of legal forms generated by software are also at risk.[329] Some commentators suggest all these problems can be avoided with a disclosure.[330] A disclosure may be sufficient to warn a nonlawyer that general statements of the

[324] Stephen Gillers, *A Profession If You Can Keep It: How Information Technology and Fading Borders Are Reshaping the Law Marketplace and What We Should Do About It*, 63 HASTINGS L J. 953, 1010-11 (2012).
[325] C.R.C.P. 220(1) (West 2012).
[326] Va. State Bar Rules of Prof'l Conduct R. 5.5.
[327] Gillers, *supra* note 249.
[328] An exception to the general rule exists in Texas. Texas took action to protect programmers of legal use software, at least those who use conspicuous disclaimers, after a Texas court found software developers, whose program was sold to help with family law disputes, to be engaged in the unauthorized practice of law. Unauthorized Practice of Law Comm. v. Parsons Tech., Inc., 179 F.3d 956 (5th Cir. 1999). Most states do not protect those who sell forms. Further, since a downloadable program can typically be obtained by residents of every state, even a Texas programmer is at risk in the forty-nine other states.
[329] For example, an insurance agent used legal-based software to generate a fill-in-the-blank form which he then filled out to help his elderly neighbor make a will. Franklin v. Chavis, 640 S.E.2d 873, 875 (S.C. 2007). After the elderly neighbor's death, her family sued Chavis for "engag[ing] in the unauthorized practice of law." The South Carolina Supreme Court found that Chavis had engaged in the unauthorized practice. "Even the preparation of standard forms that require no creative drafting may constitute the practice of law if one acts as more than a mere scrivener." *Franklin*, 640 S.E.2d at 876. *See also* Mathew Rotenberg, Note, *Stifled Justice: The Unauthorized Practice of Law and Internet Legal Resources*, 97 MINN. L. REV. 709 (2012).
[330] *See, e.g.,* Bennett, *supra* note 313, at 127 ("A lawyer may use disclaimers to reduce problems involving unauthorized practice of law [stating] the state (or states) in which the attorney is admitted. Attorneys may take the additional step of asking potential clients about their residence before answering any questions or sending any

status of the law or the existence of a variety of legal options does not create an attorney-client relationship and such generalized statements should not be relied upon. It is far more difficult to argue that the offering of a form with specific legal language for specific purposes can be protected by a disclaimer. Action that contradicts the terms of the disclaimer invalidates the disclaimer. In addition, if the operator of such a website responds to a question or request from a nonlawyer, the disclaimer provides no protection. It is not the potential client's job to self-screen based on a disclosure. Another option might be screening questions by asking the poser's residence, but if the webpage itself contains advice without further interaction, screening is not a viable option.

The bigger problem, for purposes of this Article, is not nonlawyer programmers or users. It is the involvement of lawyers in drafting the forms, assisting in the creation of the software, and making a profit of the sale of the forms. They risk the creation of an attorney-client relationship in every state, since the webpage will be available to all, and can be sued for malpractice. Again, disclaimers are a good idea to aid in the prevention of inappropriate attorney-client relationships.[331] Disclaimers must be conspicuous, easily understood, properly placed, and not misleading.[332] A District of Columbia ethics opinion puts disclaimers in context when it "reiterates 'that even the use of a disclaimer may not prevent the formation of an attorney-client relationship if the parties' subsequent conduct is inconsistent with the disclaimer.'"[333]

A professionalism creed should include the following:

---

messages."); Jordana Hausman, Current Dev., *Who's Afraid of the Virtual Lawyers? The Role of Legal Ethics in the Growth and Regulation of Virtual Office*s, 25 GEO. J. LEGAL ETHICS 575, 587-589 (2012); Stephanie L. Kimbro, *The Law Office of the Near Future*, 83 N.Y. St. B.J. 28, 30-31 (2011).

[331] *Id.*

[332] Browne-Barbour, *supra* note 146, at 571 (citing ABA Comm. on Ethics & Prof 1 Responsibility, Formal Op. 10-457, at 1-6 (2010)).

[333] D.C. Bar Ass'n, Ethics Op. 370, s*upra* note 32.

> Lawyers must recognize that a web presence is open to residents of other jurisdictions. Attorneys making specific statements of the law applicable to certain facts or answering questions online may create an attorney-client relationship. Lawyer's legal advice or software to generate legal forms online must be licensed in all applicable states or undertake measures to screen potential clients' residences. Lawyers must always ascertain the location of people with whom they electronically communicate before giving any legal advice via any electronic medium.

I. Rule 7.1: Misleading Information about a Lawyer's Services

Model Rule 7.1 states, "A lawyer shall not make a false or misleading communication about the lawyer or the lawyer's services."[334] This restriction is related to, and overlaps some with, Rules 7.2 and 7.3, discussed in the next Subpart, which directly addresses lawyer advertising, as well as Model Rule 8.4(e), discussed in Subpart III K, which addresses improper implications of influence.

Lawyers have historically used various mechanisms to mislead others about the nature or quality of their services. The internet has introduced ample additional cheap and easy opportunities for lawyers to make misleading assertions about themselves in a context that may or may not qualify as advertising. A New Jersey lawyer posted excerpts from court opinions that complimented his work. After a judge asked that his comment be taken down, the judge referred the matter the New Jersey Committee on Attorney Advertising.[335] The Committee subsequently issued a guideline forbidding the use of "a quotation or excerpt from a court opinion (oral or written) about the attorney's abilities or legal services," commenting that such statements are misleading.[336] Such conduct could also fall under Model Rule 8.4(e) by suggesting that this lawyer can exercise improper influence over the quoted judge.

---

[334] MODEL RULES OF PROF'L CONDUCT r. 7.1 (AM. BAR ASS'N 2013).
[335] David L. Hudson Jr., *Federal District Court Cautions Lawyers to Be Careful About Repeating Judges' Compliments,* A.B.A. J. (Oct 1, 2013 2:20 AM CST), http://www.abajournal.com/magazine/article/federal_district_court_cautions_lawyers_to_be_careful_about_repeating_judge/.
[336] *Id.*

A recent D.C. ethics opinion cautions lawyers to be careful in their social media posts regarding results of cases, and information on clients, "because [internet-based publications such as social media] have the capacity to mislead by creating the unjustified expectation that similar results can be obtained for others."[337]

One of the predominate features of the internet is the myriad of ways for collecting and displaying rankings, reviews, and other kinds of feedback. Many businesses and professionals, including lawyers, have hired companies that specialize in writing and posting fake online reviews of their services.[338] Fake reviews can be positive reviews that put one's own services or firm in a good light, or they can be negative reviews intended to undercut other lawyers or retaliate against a judge.

Another infamous example involves a review posted by the CEO of a Fortune 500 company, Whole Foods market.[339] He used a fictional identity to post for eight years on message boards to praise his brand and disparagement competitors. Lawyers with enough ego may well try the same scheme. For example, one small San Diego firm found itself embroiled in a suit with Yelp after allegedly soliciting fake reviews.[340] Another concern is lawyers who pay real clients to write positive reviews for them on Google or other websites. Failing to state that the reviewers are paid or receive other forms of compensation is itself misleading. Pressuring ongoing clients to write positive reviews may be perceived as a condition of continued

[337] DC Bar Ass'n, Ethics Op. 370: Social Media I: Marketing and Personal Use, Nov. 2016, http://www.dcbar.org/bar-resources/legal-ethics/opinions/Ethics-Opinion-370.cfm.
[338] Dominic Rushe, *Fake Online Reviews Crackdown in New York Sees 19 Companies Fined*, THE GUARDIAN (Sept. 23, 2013), http://www.theguardian.com/world/2013/sep/23/new-york-fake-online-reviews-yoghurt?commentpage=1.
[339] *Sockpuppet (Internet)*, WIKIPEDIA, http://en.wikipedia.org/wiki/Sockpuppet_%28Internet%29 (last visited Sept. 20, 2014).
[340] Brian Focht, *Astroturfing: Fake Online Reviews are Bad News for Law Firms*, A.B.A., http://www.americanbar.org/content/dam/aba/publishing/rpte_ereport/2013/5_october/astroturfing.authcheckdam.pdf (last visited Mar. 27, 2017). Eventually, this case settled. Cyrus Farivar, *Yelp settles suit with bankruptcy lawyer over allegations of fake reviews*, ARSTECHNICA (Oct. 2, 2015, 4:20 PM), https://arstechnica.com/tech-policy/2015/10/yelp-settles-lawsuit-with-bankruptcy-over-allegations-of-fake-reviews/.

representation and such reviews are not voluntary and thus their content is misleading.

As discussed in the next Subpart, each jurisdiction may have slightly different rules about lawyer advertising that implicate testimonials. Some states do not allow testimonials or online reviews at all, which can cause problems for lawyers who use LinkedIn.[341] Some states "prohibit[] comparisons to other lawyers' services, unless substantiated by verifiable objective data."[342] A client writing a review on a lawyer's page that says a particular lawyer is "the best trial lawyer in town" would be a violation of the rules because it is a prohibited comparison.[343]

One unusual twist arose in a recent case involving a California lawyer who posted on her webpage photoshopped pictures of herself and various important politicians and celebrities including Barack Obama, Arnold Schwarzenegger, and Ellen DeGeneres.[344] The disciplinary body treated these photos as a method of making herself seem more important and connected than she really is.[345] Similarly, such photos could suggest that she has improper influence with powerful government actors and may be willing to use that influence on behalf of a client.[346]

Standards could include a provision that looks like this:

> Lawyers should be wary of quoting out of content excerpts from court opinions that mention the quality or nature of a lawyer's services since such statements may be misleading. Further, lawyers may not pay for online reviews or pressure clients to write reviews during an ongoing representation. Lawyers may never misrepresent their identities or write reviews of their own services online as such conduct is clearly misleading. Finally, lawyers should never use technology to misrepresent their legal services, their influence in the community, or their

[341] Smith, *supra* note 54, at 7.
[342] *Id.*
[343] *Id.*
[344] Paul Vercammen, *California Attorney Facing Suspension for Fake Photos with Celebs*, CNN (Sept. 20, 2014, 1:10 AM), http://www.cnn.com/2014/09/19/us/california-lawyer-suspension-fake-celebrity-photos/index.html?c=us.
[345] *Id.*
[346] *See* MODEL RULES OF PROF'L CONDUCT r. 8.4(e) (AM. BAR ASS'N 2013) ("It is professional misconduct for a lawyer to . . . state or imply an ability to influence improperly a government agency or official or to achieve results by means that violate the Rules of Professional Conduct or other law."). A more interesting question involves the lawyer who has authentic pictures of herself with various famous and powerful people, including judges. And consider the lawyer who includes on her Facebook page a picture of her and the judge for whom she clerked in a friendly embrace.

reputation.

J. Rules 7.2 and 7.3: Restrictions on and Requirements of Advertising

Rules 7.2 and 7.3 on advertising and solicitation of clients have been amended to refer to "electronic communication" along with other written and recorded communication.[347] Rule 7.3 refers to "real-time electronic contact" along with in-person and telephone contact.[348] Although lawyers may advertise through any kind of medium, Rule 7.2 provides in pertinent part that, "Any communication made pursuant to this rule shall include the name and office address of at least one lawyer or law firm responsible for its content."[349] Lawyers wanting to garner clients will most likely display their name. Whereas office letterhead typically displays an address, social media posts or other forms of electronic communications are less likely to display an office address. Presumably, a URL or Twitter moniker is not enough.

The most obvious problem with the advertisement regulations arises with online communications that the lawyer does not recognize are "advertisements." The DC bar warns that "any social media presence, even a personal page, could be considered advertising or marketing."[350]

The California bar issued a formal opinion stating under what circumstances an attorney's postings on social media websites would be subject to professional responsibility rules and standards governing attorney advertising.[351] For example, in some states, creating a LinkedIn

[347] MODEL RULES OF PROF'L CONDUCT r. 7.2, 7.3 (AM. BAR ASS'N 2013).
[348] *Id.* at r. 7.3.
[349] *Id.* at r. 7.2(c).
[350] D.C. Ethics Op. 230.
[351] Bar Calif. Stand. Committee Prof. Resp. & Conduct Formal Op. No. 2012-186, http://ethics.calbar.ca.gov/Portals/9/documents/Opinions/CAL%202012-186%20%2812-21-12%29.pdf (listing through hypotheticals the circumstances when a blog post by a lawyers falls within the ethics rules covering advertising and state fair advertising laws).

profile with testimonials is a violation of advertising rules.[352] Similarly, talking about case results on Twitter out of context may be deemed as soliciting services.[353] Webpages and blogs, like newsletters, largely consisting of "mundane advice" but including information on the lawyer's practice areas and contact information are advertisements.[354]

An interesting issue was raised by a firm that gave out free t-shirts with the firm logo and offered entry in a drawing for a prize to anyone who posted a picture on Facebook of themselves wearing the firm's t-shirt.[355] The ABA Commission determined that such a promotion pushed the lines of advertising and might violate existing ethics rules.[356] One enterprising firm posted advertisements for their law services on the bulletin boards of thousands of online news groups.[357] People in 140 different countries, some of which had laws prohibiting advertising by lawyers, viewed the advertisement.[358] What seemed like an enterprising idea was not carefully considered.

For intentional advertising, lawyers should make certain that their social media advertisements comply with all applicable state rules.[359] Some states may require keeping a copy of all social media posts for three years,[360] or giving the name and office address of the responsible lawyer or firm in the post itself.[361] In Connecticut, "even a simple LinkedIn invitation to another user that links to a lawyer's personal page describing his practice may be an

[352] G.M. Filisko, *The Ethics of Online Advertising*, A.B.A. (Mar. 3, 2013), http://abaforlawstudents.com/2013/03/03/ethics-online-advertising/.
[353] *Id.*
[354] *See* Debra Cassens Weiss, *A $4.2M Mistake? Lawyer is liable for faxing 'mundane advice' to accountants, 7th Circuit Says*, A.B.A. J. (Sep 16, 2013, 4:30 AM), http://www.abajournal.com/news/article/a_4.2m_mistake_lawyer_is_liable_for_faxing_mundane_advice_to_accountants.
[355] Lackey & Minta, *supra* note 127, at 160–61.
[356] *Id.*
[357] J. T. Westermeier, *Ethics and the Internet*, 17 GEO. J. LEGAL ETHICS 267, 291–92, 309 (2004).
[358] *Id.* at 309.
[359] Lackey & Minta, *supra* note 127, at 158.
[360] *Id.* at n.57 (citing Ariz. Comm. on Ethics & Prof'l Responsibility, Informal Op. 97-04 (1997)).
[361] *Id.* at n.58 (citing WASH. RULES OF PROF'L CONDUCT r. 7.2(c) (2006)).

advertisement subject to regulation."[362] A New York Ethics Opinion forbids law firms from listing their services under the "specialties" section of LinkedIn, because under New York ethics rules, lawyers, but not law firms can be certified as specialists.[363] The DC Bar warns that lawyers should familiarize themselves with the ethical rules for social media and online resources not just in D.C., but also in the surrounding jurisdictions, because some jurisdictions, such as Maryland and Virginia, have rules that allow for the discipline of lawyers that are not even admitted in their jurisdictions.[364]

A standards provision might look like this:

> At a minimum, lawyers need to ensure that intentional advertisements comply with local laws and rules. Lawyers should be aware that the advent of digital advertising allows them to advertise beyond state lines. As such, lawyers should be prepared to comply with regulations in other states that to which they may be subject.

K. Rule 8.2: Disparaging Judicial and Legal Officials

Rule 8.2 provides:

> A lawyer shall not make a statement that the lawyer knows to be false or with reckless disregard as to its truth or falsity concerning the qualifications or integrity of a judge, adjudicatory officer or public legal officer, or of a candidate for election or appointment to judicial or legal office.[365]

A famous example illustrating the need for his rule involves a lawyer speaking on a talk show—although the same communication could just as easily have been made online. The

---

[362] *Id.* (citing Martin Whittaker, *Internet Advertising Isn't Exempt from Rules, Speakers Make Clear in Separate Programs*, 24 L. MANUAL OF PROF. CONDUCT 444, 444-45 (2008)); *see also*, Mason Gordon & Alex Derstenfeld, *The LinkedIn Lawyers: The Impact of Article 145 of the Code of Professional Conduct of Lawyers on Social Media Use*, LEXOLOGY (July 19, 2016), http://www.lexology.com/library/detail.aspx?g=5b784395-91b3-4274-a964-a587dc34807e (noting that multiple authors have argued that LinkedIn constitutes an advertising platform).

[363] Debra Cassens Weis, *Law Firms Can't Describe 'Specialties' on LinkedIn, New York Ethics Opinion Says*, A.B.A. J. (Aug 16, 2013 11:25 AM CDT), http://www.abajournal.com/news/article/law_firms_cant_describe_specialties_on_linkedin_new_york_ethics_opinion_say; *Accord* D.C. Bar Ethics Opinion 370, *supra* note 32 (noting that although "jurisdictions, like New York, do not permit lawyers to identify themselves as "specialists" unless they have been certified as such by an appropriate organization. They are, however, permitted to detail their skills and experience.").

[364] *Id.*

[365] MODEL RULES OF PROF'L CONDUCT r. 8.2(a) (AM. BAR ASS'N 2013).

lawyer "declare[d] war" on three court of appeals judges calling them "jackass[es]" and compared them to Adolf Hitler and other Nazis.[366] Another lawyer on his blog called a particular judge an "EVIL, UNFAIR WITCH," who "is clearly unfit for her position and knows not what it means to be a neutral arbiter."[367]

Aside from a lack of civility, such comments erode public confidence in the legal system and profession. First, most readers may well believe that at least some toned-down version of the allegations is factual. Second, many readers could perceive the legal system as an ugly joke rather than a serious place to resolve disputes. Although lawyers are free to criticize judicial opinions in public, such criticisms should be professional and not personal. In recent years, the climate of public discourse has so coarsened that public criticism of judges' competency and neutrality has become center stage.[368]

Language in a bar association's standards might look like this:

> Lawyers may openly criticize judicial opinions. However, such criticisms should always be professional and never a personal attack on the person, or the competence and bias of the judge. Such criticisms damage the credibility of the lawyer and bring the profession into disrepute. If the behavior of a judge is subject to dispute, lawyers should refer to matter to the appropriate regulating authority and avoid public disclosure.

L. Rule 8.4: Maintaining the Integrity of the Profession

1. Rule 8.4(c): Fraud and Deception

Rule 8.4(c) offers a general statement advising lawyers to avoid dishonesty in all its forms. It states: "It is misconduct for a lawyer to engage in conduct involving dishonesty, fraud, deceit or misrepresentation." As discussed elsewhere, many types of technoblunders involve misleading

[366] Grievance Adm'r v. Fieger, 719 N.W.2d 123, 129 (Mich. 2006).
[367] John Schwartz, *A Legal Battle: Online Attitude vs. Rules of the Bar*, N.Y. TIMES, Sept. 12, 2009, at A1, http://www.nytimes.com/2009/09/13/us/13lawyers.html.
[368] For a discussion about President's Trumps disparagement of judges and Justice Antonin Scalia's biting and sometimes personal criticisms of his colleagues, as well as other social trends that lead to rude and uncivil language within the profession, see Cheryl B. Preston, *Professionalism in the Trump Era* (forthcoming).

others. The remainder of Rule 8.4 addressed additional specifics.

2. Rule 8.4(e): Improper Implication of Influence

Rule 8.4(e) provides: "It is professional misconduct for a lawyer to . . . state or imply an ability to influence improperly a government agency or official or to achieve results by means that violate the Rules of Professional Conduct or other law."[369] This rule is directed to lawyers, but on occasion, judges lure lawyers into violations because they are not careful about their own behavior. This Subpart focuses on lawyer-judge interactions that may give the impression that the lawyer has undue influence with the judge or that the judge is biased. It discusses judges' friending and other social media relationships involving judges.[370] Judicial conduct and technology has received focused attention from the ABA.[371]

Issues relating to lawyers' friending in the course of factual research are discussed in Subpart III D. Friending as a form of ex parte communications is discussed in Subpart III F. Issues relating to the advertising and friending as discussed in Subpart III H and I.

A lawyer who is friends with or following a judge may use that fact to create the appearance of improper communications or relationships suggesting judicial bias.[372] Such relationships may create an impression that the judges favor such attorneys or that the attorneys "are in a special position to influence the judge."[373] Such is why a Florida judge was disqualified in a criminal case when it was discovered that the judge was Facebook friends with the

[369] MODEL RULES OF PROF'L CONDUCT r. 8.4(e) (AM. BAR ASS'N 2013).
[370] For detailed discussions of judges' social media behavior, see John G. Browning, *Why Can't We Be Friends? Judges' Use of Social Media*, 68 U. MIAMI L. REV. 487 (2014), and David Hricik, *Bringing a World of Light to Technology and Judicial Ethics*, 68 U. MIAMI L. REV. 487 (2024-25).
[371] ABA Formal Op. 462, *supra* note 16 ("The judge should not form relationships with persons or organizations that may violate Rule 2.4(c) by conveying an impression that these persons or organizations are in a position to influence the judge.").
[372] The ABA's Model Code of Judicial Conduct states that, "A judge shall act . . . in a manner that promotes public confidence in the independence, integrity, and impartiality of the judiciary. . . ." MODEL CODE OF JUDICIAL CONDUCT r. 1.2 (AM. BAR ASS'N 2011).
[373] Facebook: Using Social Networking Web Site, CJE Opinion No. 2011-6, 2011 WL 7110317, at *3.

prosecutor.[374]

Attitudes differ on judges and friending.[375] Most official ethics opinions that address the issue do not condemn friending as *per se* improper.[376] However, in a few states, ethics opinions state that lawyer-judge friending is prohibited.[377] Whether or not judges should be allowed to "friend" lawyers, the mere presence of an online friendship can produce a variety of ethical problems.[378] A Staten Island judge was transferred because he friended lawyers on Facebook, and the lawyers complained.[379] A Florida judge was removed from a divorce case because she friended one of the parties.[380] The litigant did not accept the friend request, and she feared that this offended and biased the judge against her.[381] In another example, a trial judge who sent a "friend" request to one the parties in a divorce case was disqualified because sending the request

[374] Domville v. State, 103 So. 3d 184, 185 (Fla. Dist. Ct. App. 2012); *see also* State v. Thomas, 376 P.3d 184, 198 (N.M. 2016) (cautioning against "friending" that can be misconstrued and "create an appearance of impropriety"); Debra Cassens Weiss, *Judge reprimanded for friending lawyer and googling litigant,* A.B.A. J. (June 1, 2009 12:20 PM), http://www.abajournal.com/news/article/judge_reprimanded_for_friending_lawyer_and_googling_litigant/.

[375] CHARLES GARDNER GEYH, JAMES J. ALFINI, STEVEN LUBET & JEFFREY M. SHAMAN, JUDICIAL CONDUCT AND ETHICS § 10.05E (Lexis Nexis, 5th ed. 2015). *Compare* Samuel Vincent Jones, *Judges, Friends, and Facebook: The Ethics of Prohibition*, 24 GEO. J. LEGAL ETHICS 281, 297 (2011) ("Whenever a judge permits [a social media] user to be a 'friend,' the judge risks violating this ethical standard because a potential consequence of [social media] 'friending' is that the [social media] user could use the [social media] 'friendship'" with the judge to advance his or her personal or financial interest.) *with* Bill Haltom, *If You Are a Judge, You Better Get a Dog*, TENN. B.J., Feb. 2010, at 36 (offering a humorous rebuttal to the notion that "friending" between judges and lawyers is unprofessional and damaging).

[376] *See Judicial Ethics Advisory Opinions on Social Media*, NAT'L CENTER FOR ST. COURTS, http://www.ncsc.org/Topics/Media/Social-Media-and-the-Courts/State-Links.aspx?cat=Judicial%20Ethics%20Advisory%20Opinions%20on%20Social%20Media (last visited Aug. 5, 2013); *see, e.g.*, ABA Formal Op. 462, *supra* note 16 ("Because of the open and casual nature of [social media], a judge will seldom have an affirmative duty to disclose a [social media] connection."). For other state's advisory opinions on this issue, see Az. S. Ct Jud. Ethics Advis. Comm., Use of Social And Electronic Media By Judges And Judicial Employees Adv. Op. 14-01, at 14 (revised August 5, 2014), https://www.azcourts.gov/LinkClick.aspx?fileticket=zNRP1_l8sck%3D&portalid=137.

[377] *Judicial Ethics Advisory Opinions on Social Media*, *supra* note 286 (Florida, Massachusetts, and Oklahoma opinions state that judges may not friend attorneys that may appear in their court; California, Kentucky, Maryland, New York, and Ohio opinions state that judges may friend attorneys that may appear in their court.).

[378] Jones, *supra* note 311, at 296.

[379] Alex Ginsberg, *Staten Island Judge Matthew Sciarrino Disciplined for Friending Lawyers on Facebook*, N.Y. POST, http://www.nypost.com/p/news/local/staten_island/si_judge_is_red_face_1TCZaxBoS2p5oOyES11jPN (last updated Oct. 15, 2009, 10:44 AM).

[380] Stephanie Francis Ward, *Judge Removed from Divorce Case after Sending One Party a Facebook Friend Request*, A.B.A. J. (Jan 29, 2014 5:40 AM), http://www.abajournal.com/news/article/judge_removed_from_divorce_case_after_party_rebuffs_facebook_friend_request/?utm_source=maestro&utm_medium=email&utm_campaign=weekly_email.

[381] *Id.*

placed the party in the position of accepting the invitation and engaging in improper ex parte communications or face the reasonable fear that rejecting the request would offend the judge.[382] Although these cases involve judges, who are subject to separate ethical rules, the rationales used in these cases may apply equally to a lawyer who accepts a friend request or who send them to other lawyers or parties in the litigation.

Aside from friending, social media posts or other forms of electronic advertising may run afoul of Model Rule 8.4(e) because lawyers post pictures of themselves with judges or quote or restate praise given them by a judge.[383] One case that reached the Federal Circuit involved a lawyer from a big firm who circulated a praise-filled email received from a former chief judge.[384] After the lawyer/recipient forwarded the email widely in connection with soliciting business,[385] the lawyer was publicly reprimanded, and the judge resigned. The court held:

> While the dissemination of complimentary comments by a judge contained in a public document would not itself constitute a violation of Model Rule 8.4(e), we conclude respondent's actions violated the rule. First, the email both explicitly describes and implies a special relationship between respondent and then-Chief Judge Rader. The text of the email describes a close friendship between the two.[386]

The lawyer may have had time to think in the process of retyping the words into an advertisement and mailing copies. But the ease of forwarding an email was too tempting.

A professionalism standard could include this language:

> Lawyers should be very circumspect in requesting other lawyers and judges to indicate relationships in social media that may suggest any improper influence or potential lack of objectivity in resolving legal disputes even if the relationship was initiated by the judge.

3. Rule 8.4(d) and Rule 8.4(g): Conduct Prejudicial to the Administration of Justice

[382] Chace v. Loisel, 170 So. 3d 802, 803–04 (Fla. Dist. Ct. App. 2014).
[383] See, for example, text accompanying notes 255-56 and 266-67 s*upra*.
[384] In re Reines, 771 F.3d 1326 (2014).
[385] *Id.*, at 1331.
[386] *Id.* at 1330.

Rule 8.4 (d) is the catchall many judges and disciplinary councils use to punish a lawyer for bad behavior that is difficult to fit under one of the more specific Model Rules. It provides: "It is professional misconduct for a lawyer to . . . engage in conduct that is prejudicial to the administration of justice." The Model Rules include a general statement requiring respectfulness in Rule 8.4(g), but the issue of civil discourse justifies more targeted attention.

a. Rude, Crude, and Inhumane Descriptions of Participants in the Legal System

Lawyers are sometimes crude and brutal in traditional written communications such as letters. This kind of language is often expressly covered by stated professional standards. The temptation to use disrespectful and vulgar language seems to be heightened in the fast and informal context of electronic communications. Even though mediums such as email invite offhanded and uncensored explosions and vitriol, hopefully lawyers can recognize that incivility in any communication to opposing counsel is subject to professionalism constraints. Examples abound. For instance, a lawyer in Ohio sent e-mails to the older brother of the opposing party, a pro se litigant, insulting and demeaning the entire family's gene pool and calling the opposing party an "'anencephalic cretin' with a 'single operating brain cell' whose 'brain-dead ravings' and 'anal rantings' were characteristic of the 'lunatic fringe.'"[387]

What may be less obvious are communications not intended to be seen by anyone other than those working on the case, or maybe family and friends. It has become increasingly easy and tempting for lawyers to criticize anyone—even their own clients—online, not realizing the implications of the online medium. In one instance, Steve Regan, an attorney at the Pittsburg office of Reed Smith, a big law firm, wrote on the Twitter feed of SCOTUSblog, which he mistakenly believed was the blog of the Supreme Court, "Don't screw up this like ACA

[387] Butler Cty. Bar Ass'n v. Foster, 794 N.E.2d 26, 26 (Ohio 2003).

[Affordable Care Act aka Obamacare]. . . ."[388] After SCOTUSblog tweeted back "Intelligent life?," Regan replied: "Go f__ yourself and die." His firm eventually stated "the posting of offensive commentary or language on social media is inappropriate and inconsistent with Reed Smith's social media policy. We are addressing this matter internally."[389] In the heat of a tweet, people do not stop to think about how it will read in national news.

Even if the lawyer making the communication does not use names, context is frequently more than sufficient to reveal the targeted party. For example, an Illinois attorney lost her job when she posted in her blog about a judge referred to as "Judge Clueless." She "thinly veiled the identities of clients and confidential details of a case, including statements like, 'This stupid kid is taking the rap for his drug-dealing dirtbag of an older brother.'"[390] While she might have recognized the lack of professionalism in this language in a written letter, she did not expect her online comment to become public as it was. Even communications intended for the private use of co-workers and family can be easily saved and then forwarded.

As discussed in Part II, online comments are likely to be read by more people than intended. The person who is criticized in an electronic communication is more likely to find out about the criticism than if the lawyer had expressed the criticism in a private conversation. Beyond the personal offense suffered by the victim, the injured party may experience damage to commercial, professional, social, and personal relationships stemming from any number of third parties who may harbor negative opinions about the victim. Furthermore, electronic communications are forever. Even if something is "deleted," the email or post can be preserved by anyone who saw it before it was "deleted," and the electronic memory of the transmission can

[388] Staci Zaretsky, A Biglaw Partner's Big Twitter Meltdown, Above the Law, Oct 16, 2013, 12:58 PM http://abovethelaw.com/2013/10/a-biglaw-partners-big-twitter-meltdown/.
[389] ROLL ON FRIDAY, (Oct. 18, 2013, 12:40 PM), http://www.rollonfriday.com/TheNews/EuropeNews/tabid/58/Id/2980/fromTab/36/currentIndex/3/Default.aspx.
[390] *Id.*

be easily saved in a variety of ways.[391] In May 2017, the ABA issued Opinion 477 that noted "In the electronic world, "delete" usually does not mean information is permanently deleted, and "deleted" data may be subject to recovery. Therefore, a lawyer should consider whether certain data should ever be stored in an unencrypted environment, or electronically transmitted at all."[392] But no further guidance, standards, or advice is given.

Unfortunately, electronic mediums lend themselves to thoughtless outbursts.[393] Worse, lawyers may believe they are posting anonymously, give sway to their courser natures,[394] and then discover that their identity can be traced,[395] and their content never disappears.

A possible civility standard to address these issues might state:

> Lawyers should be respectful to all participants in the legal system and avoid vulgarity, personal insults, name calling, and other uncivil language. A lawyer should be cautious of memorializing in written electronic communications comments that are unprofessional and patently offensive regarding any person involved in a litigation or negotiation.

b. Disrespecting Opposing Counsel, Opposing Clients, and Others

Even if couched in reasonably polite wording, states have adopted standards explicitly relating to communications to opposing counsel, in addition to a general statement requiring

[391] *See infra* notes 71-74 and accompanying text.
[392] American Bar Association Standing Committee on Ethics and Professional Responsibility, Formal Opinion 477R*, Securing Communication of Protected Client Information (revised May 22, 2017), https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.authcheckdam.pdf.
[393] *See infra* notes 81-94 and accompanying text.
[394] Daniel J. Solove, *The Future of Reputation: Gossip, Rumor and Privacy on the Internet* 140 (2007) (concluding that "anonymous, people are often much nastier and more uncivil in their speech [because it] ... is easier to say harmful things about others when we don't have to take responsibility"); Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to The First Amendment in Cyberspace*, 104 Yale L. J. 1639, 1642-43 (1995) (noting anonymous or pseudonymous postings "relieve[] their authors from responsibility for any harm that may ensue [and that] ... [t]his often encourages outrageous behavior without any opportunity for recourse to the law for redress of grievances"); McIntyre v. Ohio Elections Commission, 514 U.S. 334, 382 (1995) (Rehnquist, C.J., joined by Scalia, J., dissenting) ("[A] person who is required to put his name to a document is much less likely to lie than one who can lie anonymously" and that anonymity "facilitates wrong by eliminating accountability").
[395] *See infra* note 51 and accompanying text.

lawyers to treat all others with dignity.[396] Specifically, some standards forbid: imputing improper motives to an adversary without a factual basis; embarrassing or personally criticizing another attorney; attributing a position not taken to an adversary; and impugning an adversary's character, intelligence, or morals.[397] Online, lawyers sometimes make disrespectful statements about other lawyers and participants in the legal system in communications directed to third parties. Nonetheless, the target often discovers the communications directed to others. Even if undiscovered by the target, such postings can poison the well for judges, jurors, and the public who are exposed to the post. In one example, the lawyer may have believed his email to opposing counsel seemed innocuous or even humorous at the time, but the Missouri Supreme Court found it to be a violation of Model Rule 8.4(d).[398] After a contested hearing, the lawyer sent the following email: "Rumor has it that you are quite the gossip regarding our little spat in court. Be careful what you say. I'm not someone you really want to make a lifelong enemy of, even though you are off to a pretty good start."[399]

While the target of the criticism may deserve reprimand, the lawyer involved in a particular case should not be making judgment in an effort to intimidate, harass, or demean others involved in the suit. In a heated and pending domestic dispute, the attorney for the mother sent an email directed to the father's attorney reciting details of his daughter's drug dealing in a dangerous neighborhood and suggesting the father should take more seriously his daughter's behavior.[400] The recipient's wife (who, coincidentally, was also an attorney) read the email and

[396] Twenty-two states have adopted at least one of these standards urging respect towards other attorneys. Preston & Lawrence *supra* note 11, at tbl.4, 5.
[397] *Id*.
[398] *In re* Eisenstein, 485 S.W.3d 759, 763 (Mo. 2016) (en banc).
[399] *Id*. at 761.
[400] *In re* Anonymous Member of the South Carolina Bar, 392 S.C. 328 (2011). The email text reads: "I have a client who is a drug dealer on [] Street down town [sic]. He informed me that your daughter, [redacted] was detained for buying cocaine and heroin [sic]. She is, or was, a teenager, right? This happened at night in a known high crime/drug area, where alos [sic] many shootings take place. Lucky for her and the two other teens, they weren't

reported the sending attorney for discipline.[401] The Supreme Court of South Carolina issued a private letter of caution,[402] and dismissed sending attorney's claim that the bar's civility oath was an unconstitutional limit on his First Amendment rights.[403] Litigants do have a First Amendment right to be tacky, but lawyers cannot similarly conduct themselves in this way under the professionalism and civility constraints of the profession. Allowing egregious incivility to persist under the banner of freedom of speech would be a disservice to the profession. The South Carolina Supreme Court put it this way:

> The State has an interest in ensuring a system of regulation that prohibits lawyers from attacking each other personally in the manner in which [the sending attorney] attacked [the receiving attorney]. Such conduct not only compromises the integrity of the judicial process, it also undermines a lawyer's ability to objectively represent his or her client.[404]

Lawyers are asked to report to the relevant bar association misconduct of other lawyers, and doing so through the established system is an appropriate way to seek improvement in the legal profession. However, a malicious online attack on an individual lawyer or firm is inappropriate. A judge or bar association at least, can request and receive evidence, and may refuse to take any action against the allegedly misbehaving attorney if there is not enough evidence to prove liability. The public, however, cannot request or receive evidence and may not be as careful about refraining from punishing a lawyer for unsubstantiated claims. Members of the public may choose not to go to a certain lawyer or firm based on malicious information they

---

charged. Does this make you and [redacted] bad parents? This incident is far worse than the allegations your client is making. I just thought it was ironic. You claim that this case is so serious and complicated. There is nothing more complicated and serious than having a child grow up in a high class white family with parents who are highly educated and financially successful and their child turning out buying drugs from a crack head at night on or near [] Street. Think about it. Am I right?"

[401] *Id.*
[402] *Id.*
[403] *Id.*
[404] *Id.*

found online about that lawyer or firm, and thus the attacked firm or lawyer can lose clientele, even if the attack was unsubstantiated or completely false.

Last year a lawyer sued the former spouse of a divorce client because he wrote a negative review of the lawyer on Google Plus. The review said the lawyer worked for an "ethically shaky law firm."[405] The former spouse was not a lawyer, but such comments could be posted by lawyers who falsely believe they are acting with anonymity. The perception that lawyers are lacking in moral and competency qualities by attacking, insulting, or demeaning others online erodes the public's faith in the legal system.

c. Creation, Use, and Storage of Improper Electronic Content

In addition to the sex discrimination implications, some behaviors involving sexually explicit materials bring the profession into disrepute and often these behaviors involve the internet. For instance, one would imagine that lawyers recognize that using electronic communications to request sexual services as pay is inappropriate, but not everyone gets the message.[406] Another lawyer persistently pressured in a series of emails a third-year law student who had worked for him for only a few weeks to provide sexual favors as a condition of keeping her job.[407]

One East Texas chief judge deleted his social media information and resigned rather than give up his records or produce his phone in an investigation of sexting allegations.[408] He claims he gave his phone to "charity."[409] While serving in his official capacity as vice chairman of the

[405] Steve Miller, *Naperville Lawyer Sues Man Over Negative Comments Online*, CBS CHICAGO, (Sept. 19, 2013 7:57 AM) http://chicago.cbslocal.com/2013/09/19/naperville-lawyer-sues-man-over-negative-comments-online/.
[406] *See* Amanda Griffin, *Texas Lawyer Accused of Sending Inappropriate Texts*, J.D. JOURNAL, November 9, 2016, http://www.jdjournal.com/2016/11/09/texas-lawyer-accused-of-sending-inappropriate-texts/.
[407] Amanda Griffin, Texas Lawyer Accused of Sending Inappropriate Texts, J.D. Journal, November 9, 2016, http://www.jdjournal.com/2016/11/09/texas-lawyer-accused-of-sending-inappropriate-texts/.
[408] Smith County Judge Joel Baker resigns, TYLER MORNING TELEGRAPH, (Sept. 23, 2016 11:56 AM), http://www.tylerpaper.com/TP-Breaking/241295/smith-county-judge-joel-baker-resigns.
[409] *Id.*

State Commission of Judicial Behavior, he sent sexually explicit messages to a woman who responded to his "friending" request.[410] She employed a private investigator to pursue the matter.[411] The investigator found and turned over more than a thousand sexually explicit messages, photos, and videos, many of which were verified by a local television station.[412]

Another issue implicating this Model Rule 8.4 involves using the internet to access or store illegal or even unregulated sexually explicit content. Disciplinary actions have been brought against judges, district attorneys, and other governmental lawyers for excessive use of pornography on government owned computers, using government provided internet access, or on government time. In *In re Disciplinary Proceedings Against Beatse*, pornography was found on an assistant district attorney's state-provided computer.[413] An investigation ensued which found that he had been spending massive amounts of time looking at pornography.[414] He had originally lied and said that it was his son who had been looking at the pornography on his computer.[415] He also sent a number of sexual email messages to various people, including two government employees, one of whom was a court reporter.[416] Some of the emails described looking at and touching the breasts of government employees.[417] He admitted to having lied about the emails and the pornography, and he was publicly reprimanded.[418]

Some judges have been disciplined for sexually harassing or sexting staff or attorneys, even if the sexual exchanges were voluntary. In 2014, a justice on the Pennsylvania Supreme Court was ousted after sending pornographic emails to contacts in the Attorney General's

[410] Judge accused of sexting while sitting on judicial conduct board, KLTV 7, (Mar. 17, 2016, 12:05 PM), http://www.kltv.com/story/31467865/texas-judge-accused-of-sexting-while-sitting-on-judicial-conduct-board.
[411] *Id.*
[412] *Id.*
[413] *In re* Disciplinary Proceedings Against Beatse, 722 N.W.2d 385, 386–90 (Wis. 2006).
[414] *Id.*
[415] *Id.*
[416] *Id.*
[417] *Id.*
[418] *Id.*

office.[419] In another case, the court approved a stipulation for the retirement and public reprimand of a judge who was accused, along with failing to disclose a juror written communication and engaging in inappropriate conduct towards two female attorneys, of habitually viewing pornographic images on his courthouse computer.[420] The court pointed out that this caused numerous viruses to infect his computer, that personnel were exposed to the pornography when coming to repair the computer, and that the judge ignored requests to stop issued because his actions were threatening to infect the entire courthouse computer system with unwanted computer viruses.[421]

4. Rule 8.4(j): Discrimination and Prejudice

Model Rule 8.4(j) forbids a private attorney to make public comments that are racist, sexist, or that express negative group stereotypes.[422] Although few current statements of professionalism expressly warn about such bias, all bar associations should include a charge against comments that further racial, sexist, or other biases. Lesley M. Coggiola, disciplinary counsel for the South Carolina Supreme Court, reported that she has seen lawyer posts online that are degrading to various classes of people, and argues that the lawyers behind such posts should be sanctioned for "bringing the profession into disrepute."[423] She noted that one of her ongoing cases involved a lawyer's blog that she described as "vile."[424] The blog is "insulting

[419] Angela Couloumbis, *Supreme Court Suspends McCaffery Over Porn E-mails*, PHILLY.COM (Oct. 21, 2014), http://www.philly.com/philly/news/politics/20141021_Supreme_Court_votes_to_suspend_McCaffery_over_e-mails.html
[420] *In re* Downey, 937 So. 2d 643, 645-49 (Fla. 2006).
[421] *Id*.
[422] MODEL RULES OF PROF'L CONDUCT r. 8.4(g) (AM. BAR ASS'N 2016).
[423] G.M. Filisko, *You're out of Order!: Dealing with the Costs of Incivility in the Legal Profession*, A.B.A. J. (Jan. 1, 2013, 11:19 AM), http://www.abajournal.com/magazine/article/youre_out_of_order_dealing_with_the_costs_of_incivility_in_the_legal/. *See also* Christina Pajaron Skinner, *The Unprofessional Side of Social Media and Social Networking: How Current Standards Fall Short*, 63 S.C. L. REV. 241, 258 (2011) (footnotes omitted).
[424] Filisko, *supra* note 350, at 37.

everybody from Hispanics to women to 'midgets.'"[425] According to Coogiola, "technology is cited most often as the foundation for boorish behavior."[426] All the serious issues they have had, she explains, "[a]re all related to social media."[427]

Various examples abound. A lawyer at a large law firm was unveiled as having posted misogynistic lyrics online.[428] Although the poster likely believed he or she was anonymous or speaking to a close and trusted group, the posting was exposed and the poster was fired for it.[429] But the consequences do not stop there. Those who associated those lyrics with a lawyer and those who read about it in the press retain an association of such attitudes with lawyers.[430]

While online comments on message boards, social media, and emails may not immediately be seen as "public comment," the ease of spreading such comments to unintended readers and even the press argues for more explicit regulation. Such statements are detrimental to the perception of the profession and legal system. For example, underrepresented groups might be discouraged from using the legal system to resolve disputes fearing that the biases of lawyers and judges make it unlikely they will receive fair treatment. Member of the maligned group may believe that their treatment in prior cases was unfair and thus they are justified in disobeying court orders or not paying judgments.

While bias reflects poorly on all of the profession, the problem is even worse if a judge or other public official is the source of the electronic communication. Judge Cebull, a federal judge, forwarded a seemingly racist email about President Obama to some of his close friends.[431] After the email came to light, a commission investigating its impropriety uncovered many more

[425] *Id*.
[426] *Id*.
[427] *Id*.
[428] LORI ANDREWS, I KNOW WHO YOU ARE AND I SAW WHAT YOU DID: SOCIAL NETWORKS AND THE DEATH OF PRIVACY 123 (Free Press, 2011).
[429] *Id*.
[430] *See, e.g.*, *In re* Disciplinary Proceedings Against Beatse, 722 N.W.2d 385, 387–89 (Wis. 2006).
[431] Murphey, *supra* note 78.

emails laced with "disdain for African Americans, Latinos, women and various religious faiths."[432] Highlighting the problem in this case, the panel observed, "The racist and political email[s], reflects negatively on Judge Cebull and on the judiciary and undermines the public trust and confidence in the judiciary."[433]

Professionalism standards could state,

> Lawyers should not express through electronic or other media sources bigotry, prejudice, or distain for any class of people. Such behavior brings the legal profession into disrepute and weakens the confidence of the public in the fairness and efficacy of the judiciary.

IV. CONCLUSION

As the recent ABA 20/20 Commission's failures amply illustrate, the ABA cannot be expected to address the risks of technology within any reasonable time. Moreover, the Model Rules acknowledge that they do not "exhaust the moral and ethical considerations that should inform a lawyer . . . [they] simply provide a framework for the ethical practice of law."[434] Increasing pressure on the ABA to shore up the Model Rules is essential. In the meantime, however, bar associations must take action now.[435] One option is formal ethics opinions that lawyers can research by jurisdiction, if the lawyer is alert enough to ask questions. A better option is a statement of best practices standards adopted by state, local, and practice group bar associations. Professionalism creeds address a more expansive range of behavior, but most are aspirational, meaning violators are not subject to formal discipline affecting their standing to practice law. New professionalism creeds must be adopted, integrated into lawyer education, and

[432] Saba Hamedy, *Montana Federal Judge Sent Hundreds of Biased Emails, Panel Finds*, L.A. TIMES (Jan. 14, 2014, 7:30 AM), http://www.latimes.com/nation/nationnow/la-na-nn-montana-judge-racist-emails-20140118,0,2624855.story#ixzz2rMe7otTi.
[433] *Id.*
[434] MODEL RULES OF PROF'L CONDUCT pmbl. & scope ¶ 16 (2013).
[435] For a discussion of the role of law schools in the professionalism crisis and how they can take concrete steps to educate law students better, see Cheryl B. Preston, Professionalism in the Trump Era (forthcoming).

subject to enforcement. The law profession, and the society it serves, deserves a clearer statement of moral ground in technology use.

Professor Chaffee suggests that aspirational standards can be implemented "with broad moral language and a high moral tone to engage with the emotions and intuitions of those practicing law and to play upon the intuitions and emotions of those interacting with lawyers to make them believe that they are being treated fairly."[436] The importance of ensuring those who interact with lawyers believe they are being treated fairly is largely underestimated by the legal community. If the Model Rules and professionalism standards fall short of society's expectations because attorney behavior seems "intuitively wrong or elicits negative emotions," the legitimacy of the profession is threatened.[437] The lack of stated moral standards relating to an issue as important as technology and social media abuses "creates an incentive for those outside of the legal profession to begin to interfere with the self-regulation of the profession, which may have negative consequences if it is done in an unsophisticated way."[438]

As outrageous examples of attorney abuses of technology continue to make headlines, the public may form the opinion that attorney conduct is not sufficiently regulated and urge lawmakers to impose external regulation on the profession.[439] Rules backed by legislation will undoubtedly be more difficult to change and less attuned to realities of the practice than the Model Rules. The profession itself can no longer ignore lawyer abuses of technology.

---

[436] Eric C. Chaffee, *The Death and Rebirth of Codes of Legal Ethics: How Neuroscientific Evidence of Intuition and Emotion in Moral Decision Making Should Impact the Regulation of the Practice of Law*, 28 GEO. J. LEGAL ETHICS 323, 355 (2015).
[437] *Id.* at 358.
[438] *Id.*
[439] Professor Chaffee recalls how this very thing happened with business conduct in the wake of the Enron scandal. *Id.* at 358-60. Frustrated American people successfully urged Congress to pass the Sarbanes-Oxley Act of 2002; there were many regulations in the Act that addressed attorney ethics, which were previously regulated by the American Bar Association. *Id.*